サイバー犯罪の現状と対策におけるインテリジェンスの活用

日本プルーフポイント株式会社
シニアセキュリティコンサルタント
内田 浩一

proofpoint®
People-Centric Security

自己紹介

内田 浩一
シニア セキュリティ コンサルタント

GREM
CEH Certified Ethical Hacker

Malware Analysis

セキュリティベンダーにおいてマルウェア解析業務や、マルウェア検知製品の開発にも従事。

Threat Intelligence

攻撃者と脅威動向を継続的に観測し、高度なセキュリティ対策に重要なインテリジェンスの活用を支援。

SOC Supervisor

多数の大手企業や政府に対してSOCの立ち上げや運用支援のコンサルティングサービスを提供。

Penetration Testing

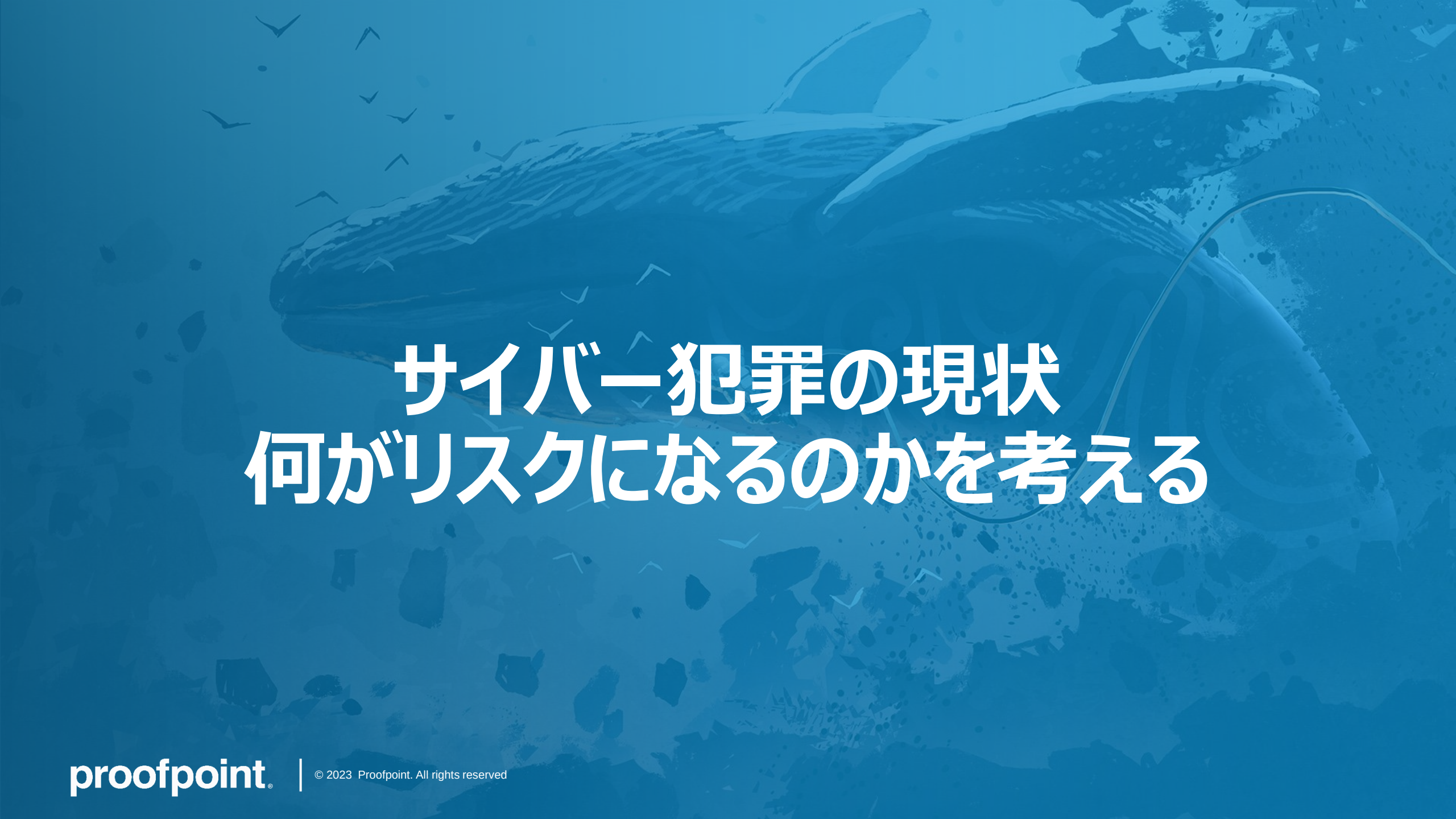
15年のPenetration test経験を有し、制御システムへの侵入やIoTデバイスに対するハッキング等、幅広い技術的検証プロジェクトをリード。

脅威分析を得意とするテクニカルコンサルタント

proofpoint

Agenda

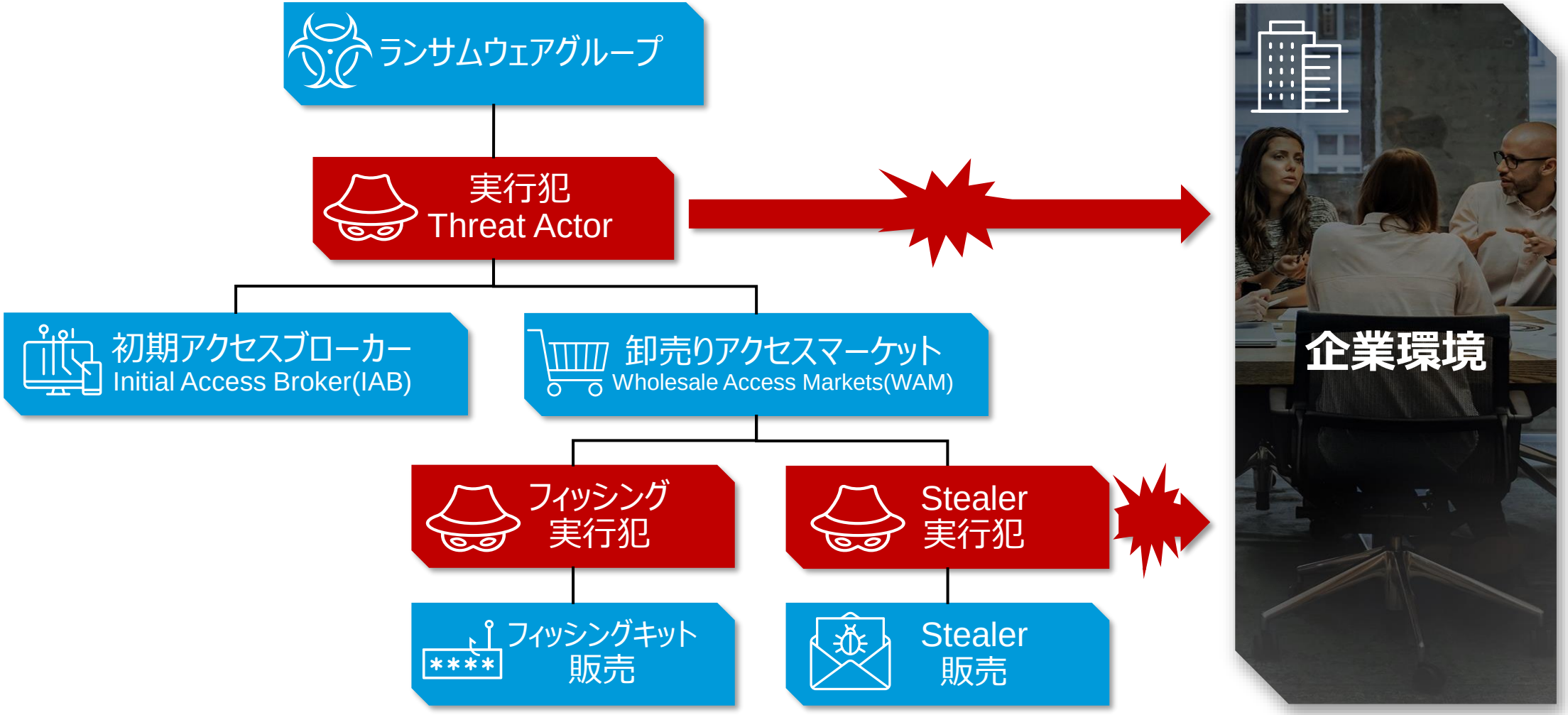
- サイバー犯罪の現状
- 攻撃の動向と手口
- 内部のインテリジェンスを活用した対策強化



サイバー犯罪の現状
何がリスクになるのかを考える

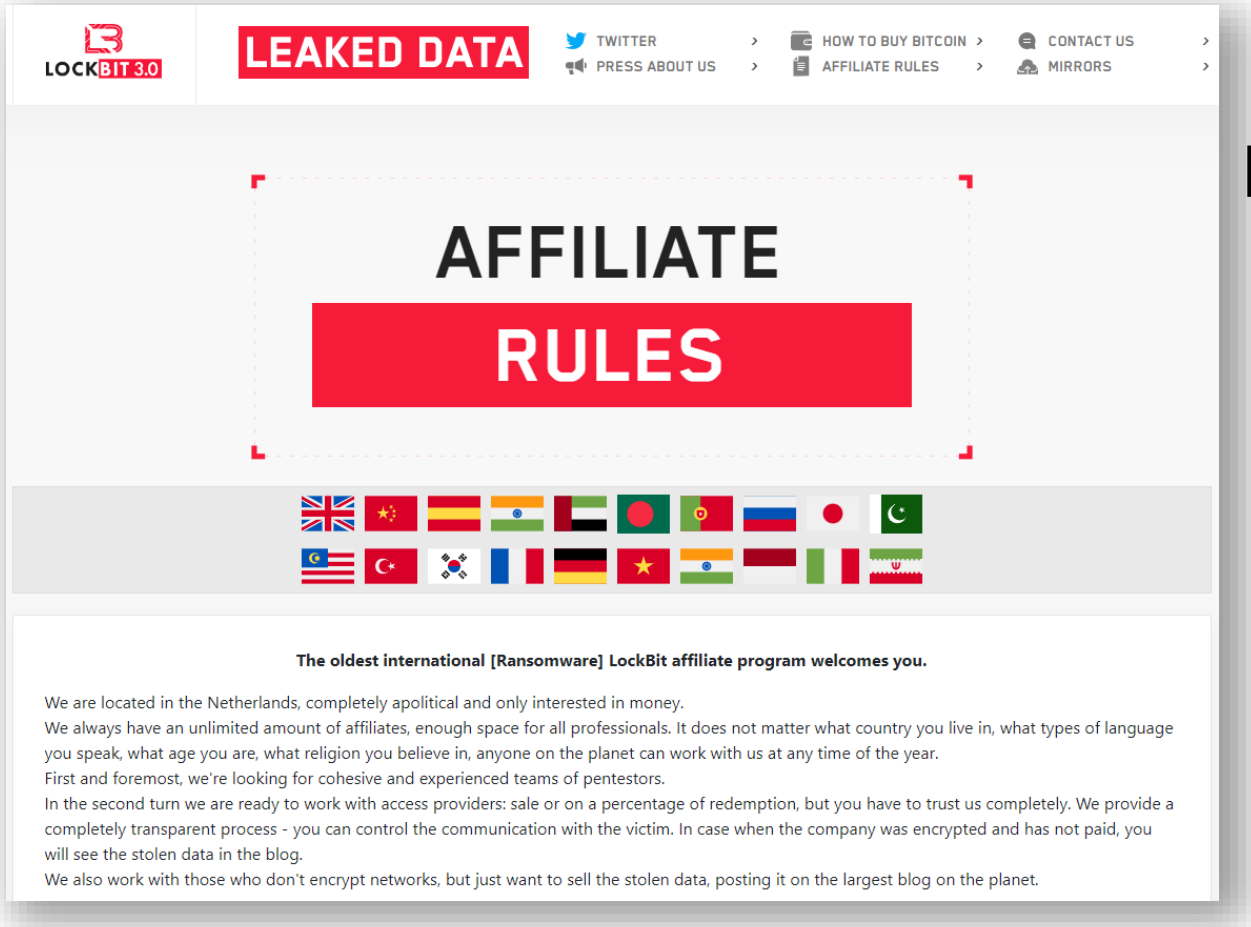
proofpoint.

サイバー犯罪エコシステム



ランサムウェアグループ

Lockbitのアフィリエイト条件



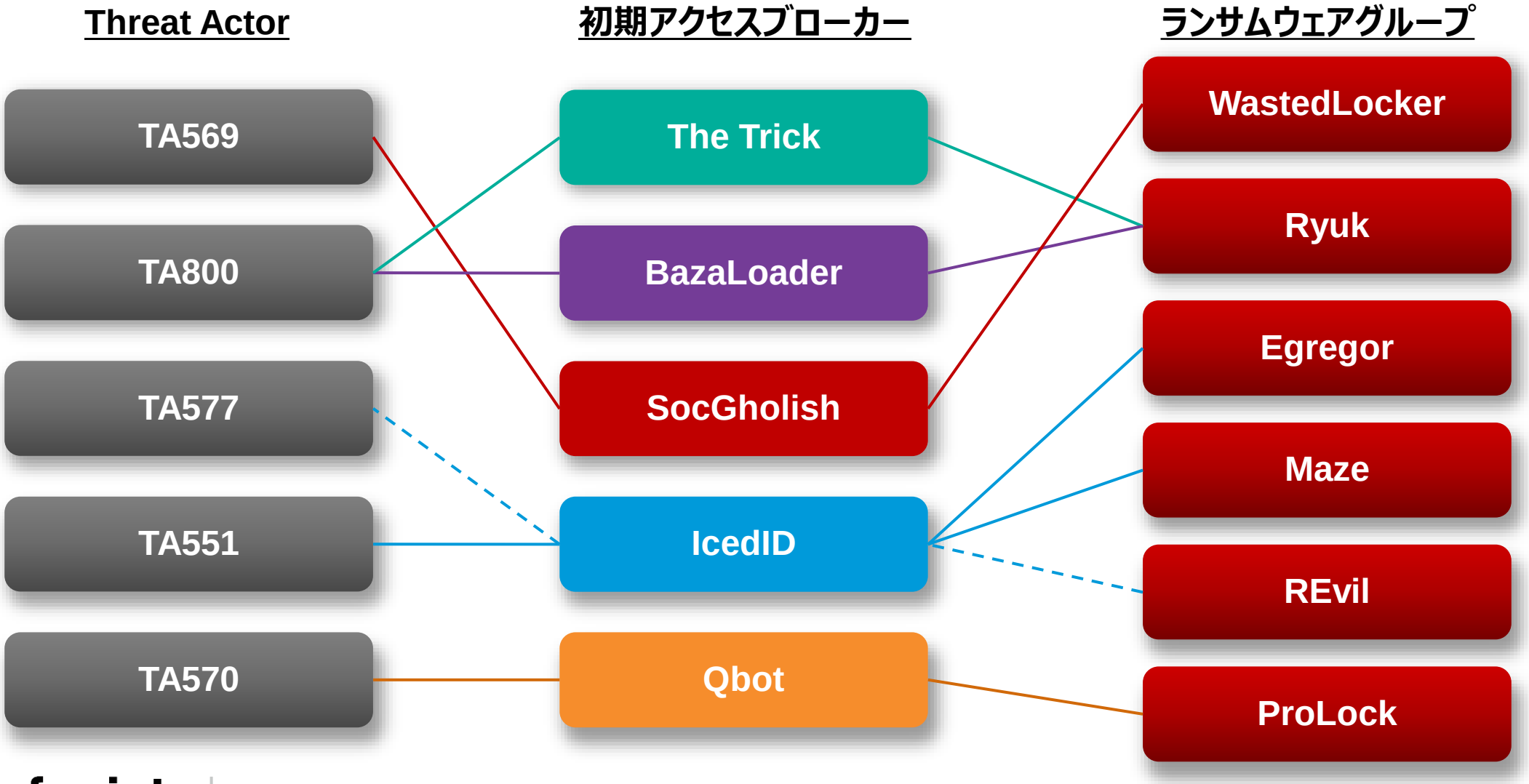
Lockbitは以下に該当する協力者を募集

- ✓ 結束力のある経験豊富なペンテスターチーム
- ✓ 初期アクセスブローカー
  - アクセス権の販売
  - 利益に対する80%の支払い

企業環境に侵入するだけのスキルを有する
ハッカーチームと協業

初期アクセスブローカーとの繋がり

初期アクセスブローカー
Initial Access Broker(IAB)

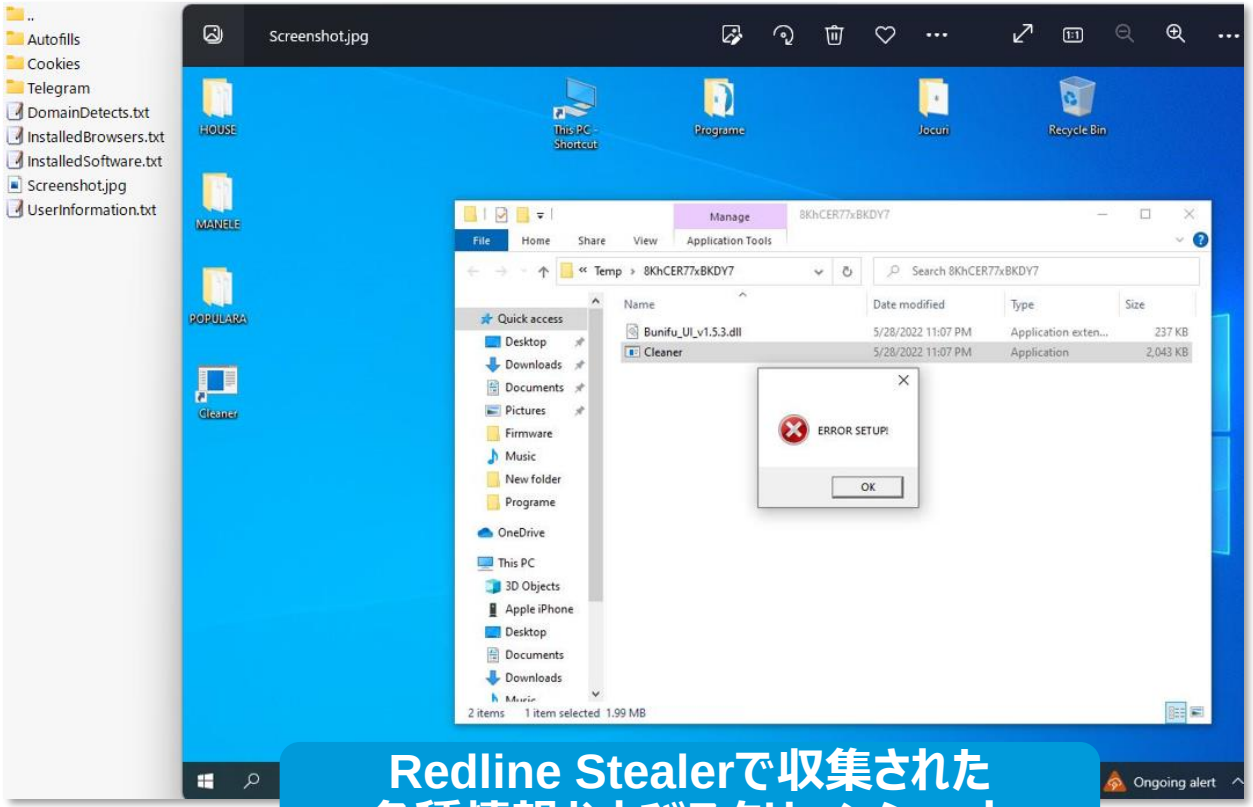


情報を販売するマーケット

卸売りアクセスマーケット
Wholesale Access Markets(WAM)

BOTS LOGS FRESH (Pages: 1 2 3 4 ... 7) by **kr00kkk**, July 28, 2022, 08:05 PM	69	5,673
100x Indian Private Logs by EvilHacker, October 2, 2022, 01:56 AM	4	663
25k passwords.txt from logs by badass2022, October 13, 2022, 08:03 AM	5	1,060
FREE RedLine stealer logs (Pages: 1 2 3 4) by **lernaean_hydra0**, July 9, 2022, 12:35 PM	35	6,193
10GB Stealer logs (Mixed) 2022 (Pages: 1 2 3 4) by **buffbyte**, June 20, 2022, 04:18 PM	39	8,908
594 STEALER LOGS 2022 FRESH by NoCry, October 1, 2022, 11:51 AM	7	597
Ruban Cloud FREE 4.36 GB FRESH LOG by **ruban**, October 13, 2022, 10:33 PM	3	617
[LOGS]MIX COUNTRIES 2022 PT3 (Pages: 1 2) by zaBrock, September 21, 2022, 07:20 AM	15	1,669
28GB redline LOGS !! GO GO TILL ITS THERE ! by ~~gruiogruev~~, October 10, 2022, 11:26 PM	7	772

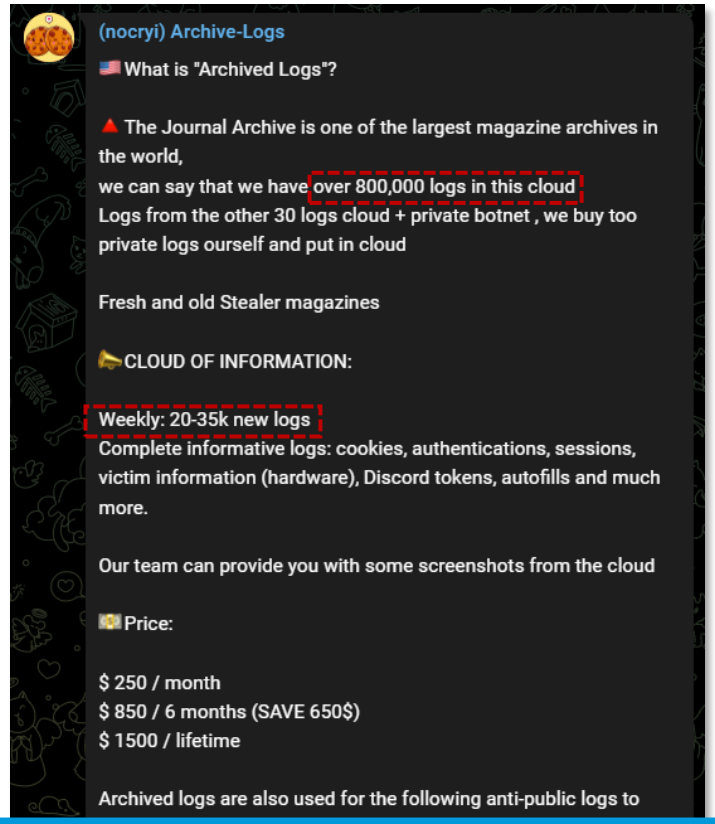
認証情報や情報窃取型マルウェアのログが多数販売されているマーケット



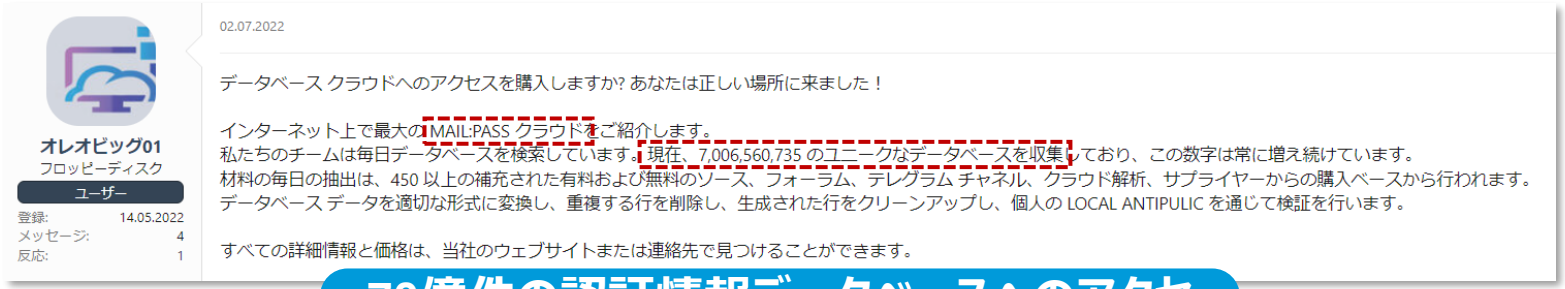
Redline Stealerで収集された各種情報およびスクリーンショット

認証情報DBのサブスクリプションサービス

卸売りアクセスマーケット
Wholesale Access Markets(WAM)

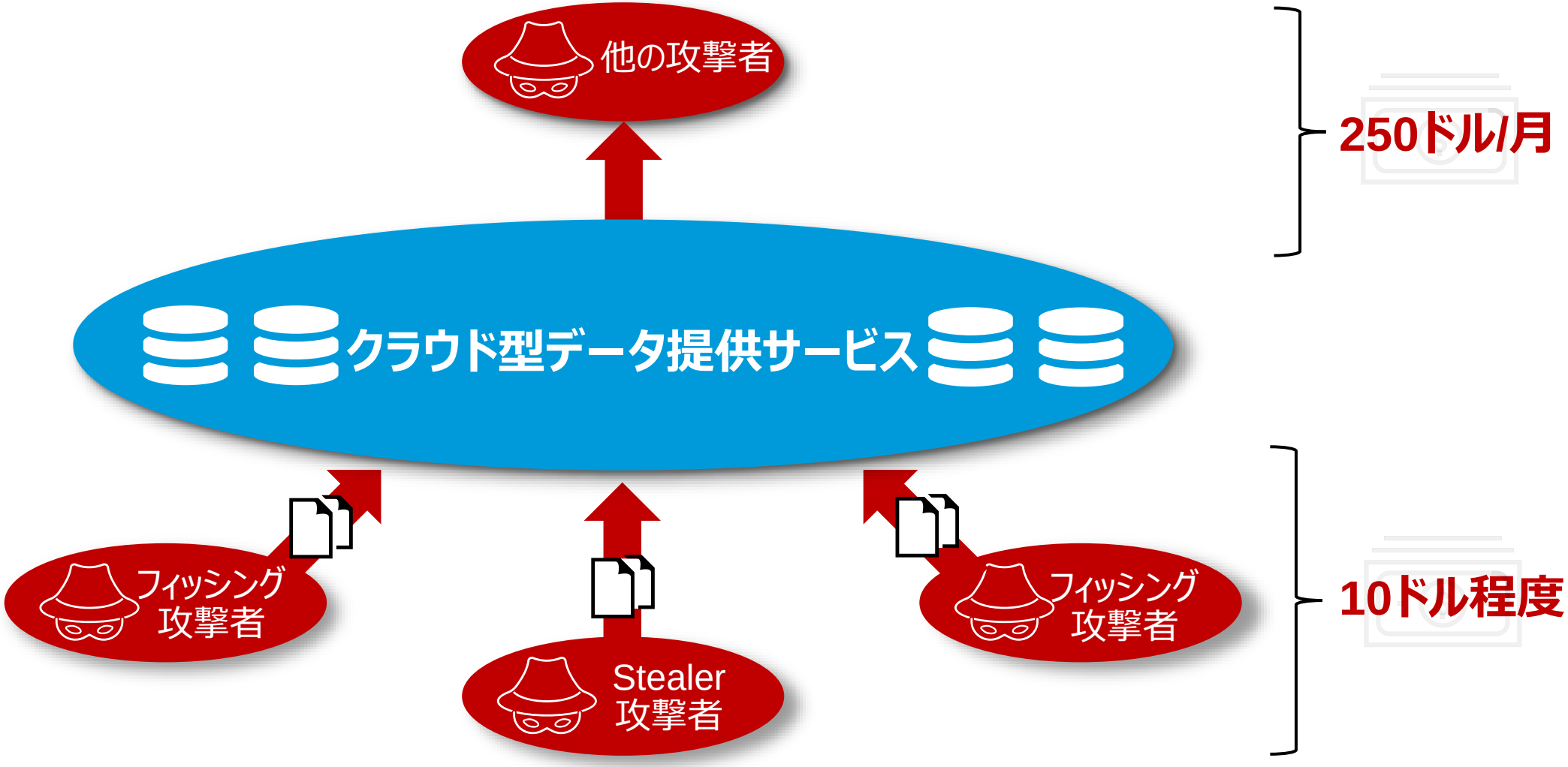


週に3万5千件新規に追加(現在80万件を保持)される情報窃取型マルウェアのログ提供サブスクリプションサービス

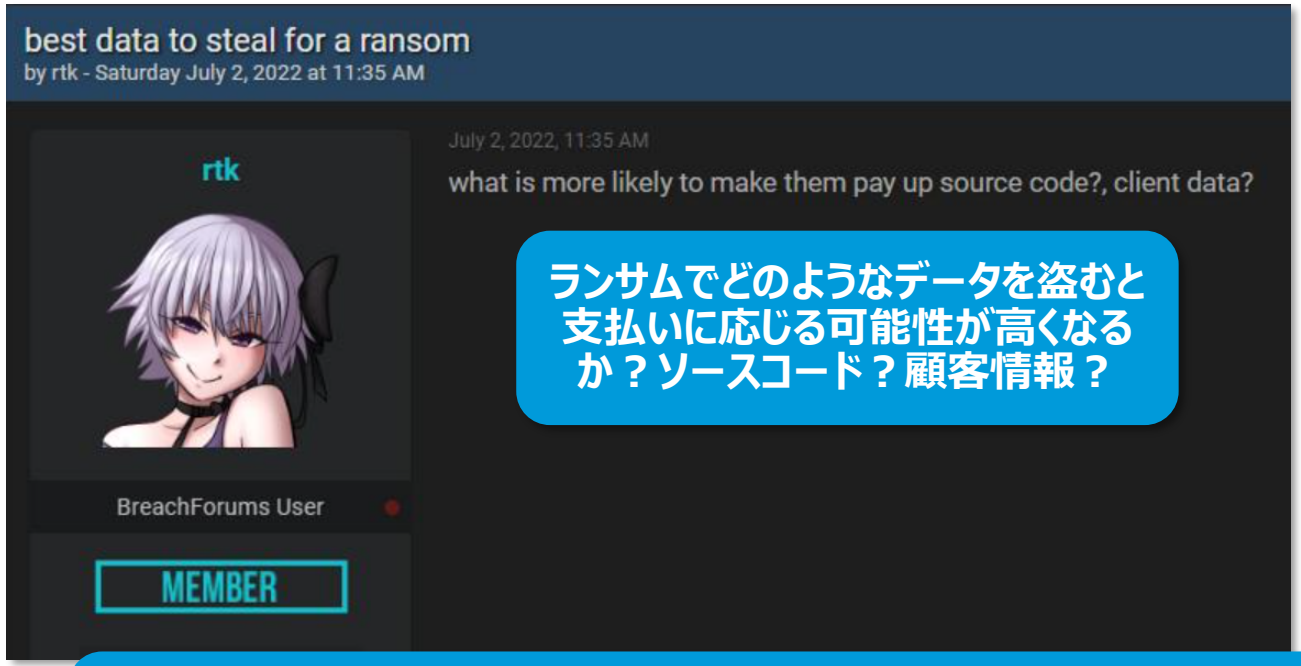


70億件の認証情報データベースへのアクセス権を提供するサブスクリプションサービス
※元はロシア語

小規模なデータ売買から大規模なサービス化へ



利益に繋がる企業は複数のグループに狙われる



ランサムでどのようなデータを盗むと
支払いに応じる可能性が高くなる
か？ソースコード？顧客情報？

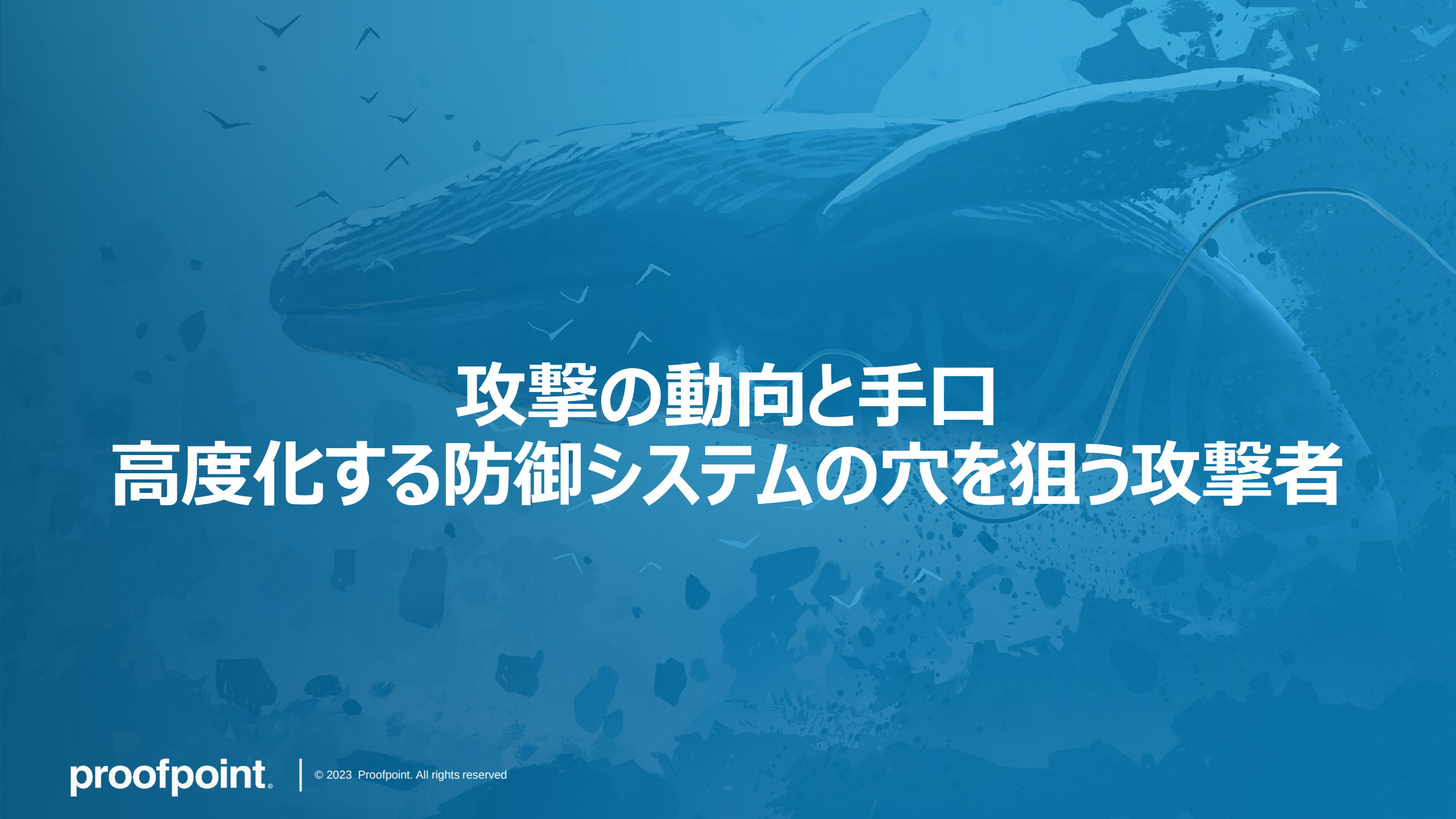
client data.

r&d yum yum

Health care data bro

health data
prison records
multimedia data of adultery, cheating

支払いの可能性が高い企業はランサムグループの標的に
サイバー犯罪もエコシステムによって効率化されているのが現状



攻撃の動向と手口
高度化する防御システムの穴を狙う攻撃者

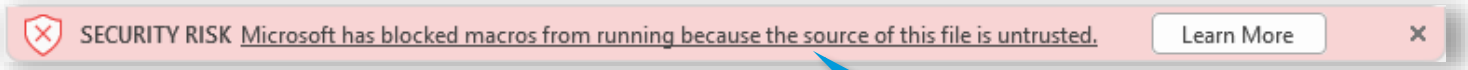
proofpoint.

脅威動向の変化に繋がった
MicrosoftがOffice製品のマクロを無効化

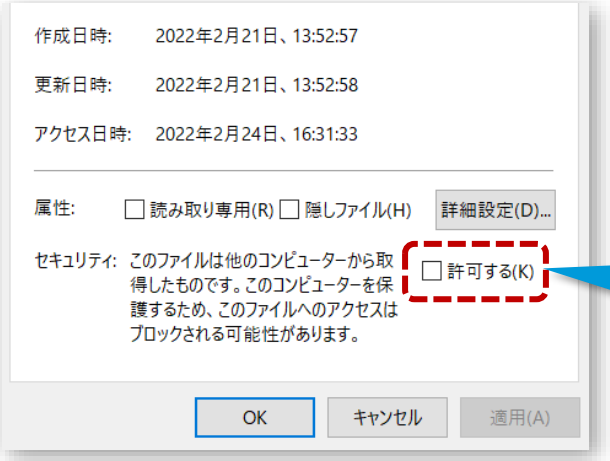
Microsoft社がマクロを無効化
- ✓ **ダウンロードしたドキュメント**のマクロを無効化
- ✓ ドキュメントを悪用した脅威に極めて有効
- ✓ 2022年4月から順次展開

脅威動向の変化
- ✓ オフィスファイルの悪用が減少
- ✓ LNKやIMG等の他ファイルへ移行
- ✓ フィッシングが激増

いままではユーザが Enable Contentをクリックする事でマクロが実行された



今後はWebやメール経由で届いたドキュメントのマクロを強制無効化



Webやメール経由で受信したファイルに対して付与する**Mark of the Web**フラグによってリスクのあるファイルを識別。

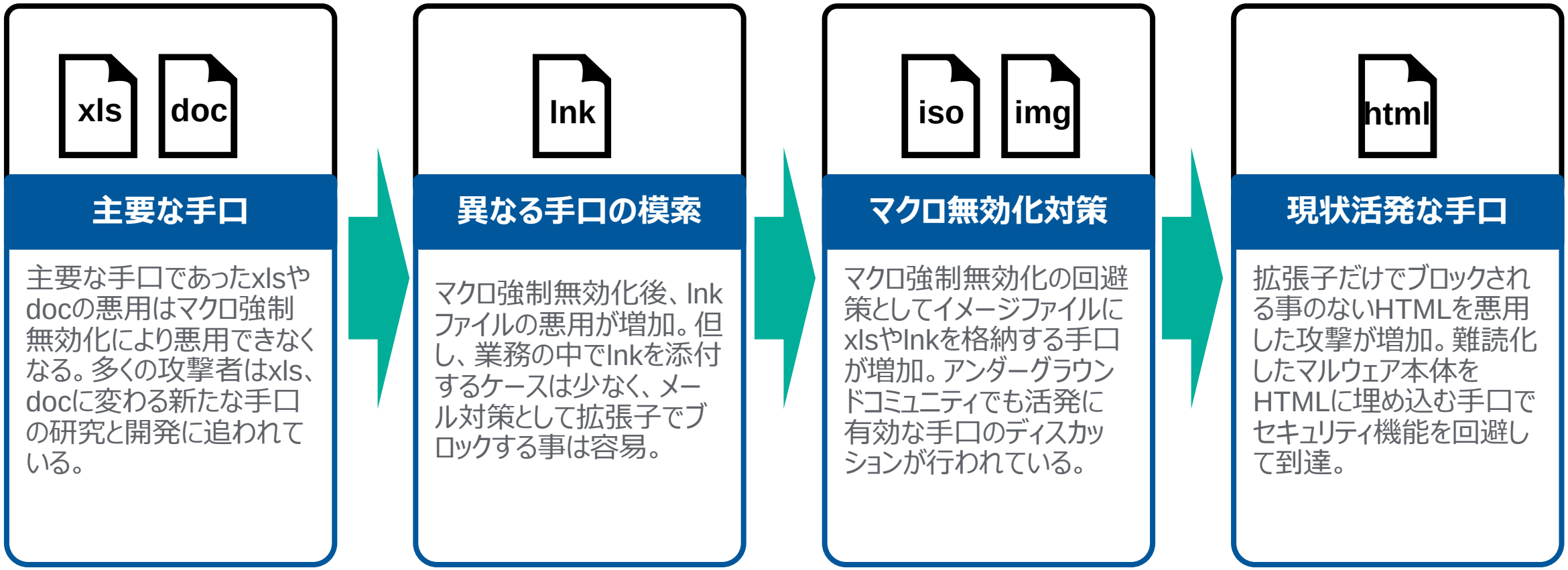
proofpoint

マクロ無効化に対するアンダーグラウンドコミュニティの動き

マクロは多くのユーザ環境で無効化されるが、いまだ多くの企業では営業や財務担当者がマクロを利用する可能性がある。入口は狭くなるが、この手口は今後も有効。

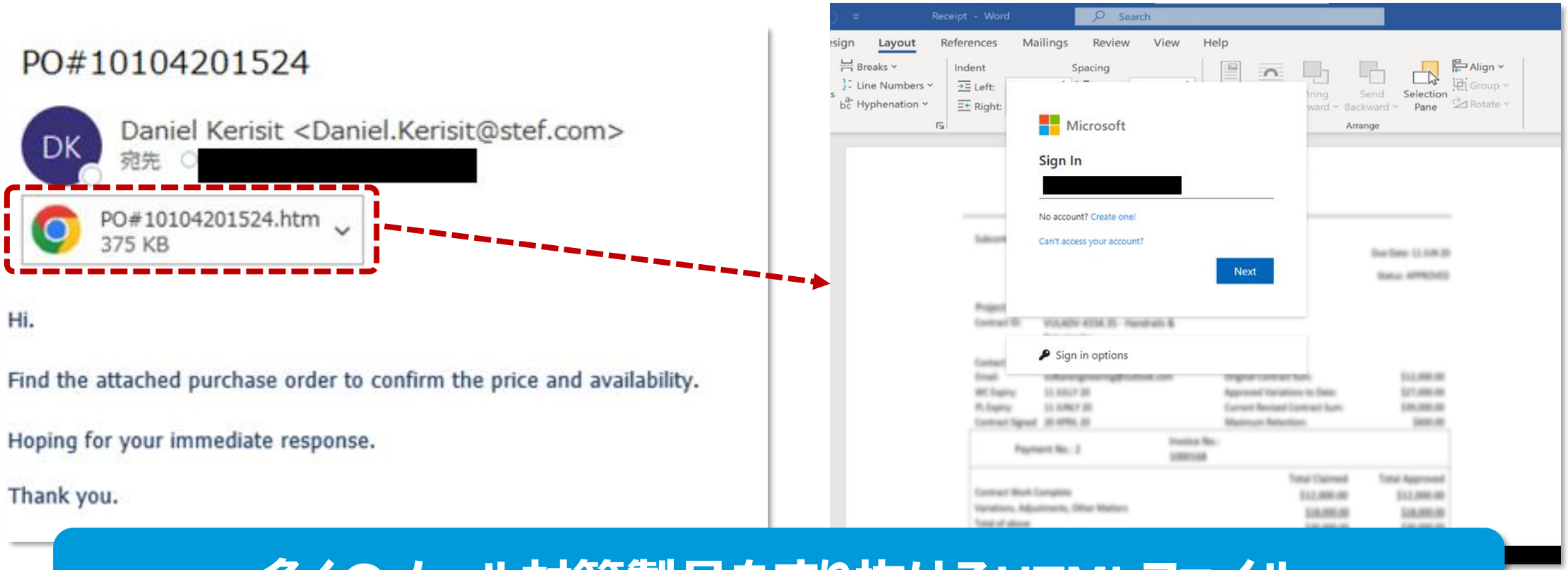
Mark-of-the-Web(ダウンロードされたドキュメント)のFlagを回避する手法が存在する為、このような手法はマクロ無効化に対抗する手段として有効。

マクロ強制無効化に対する攻撃者側の対応(2022年)



HTML添付型フィッシングの例

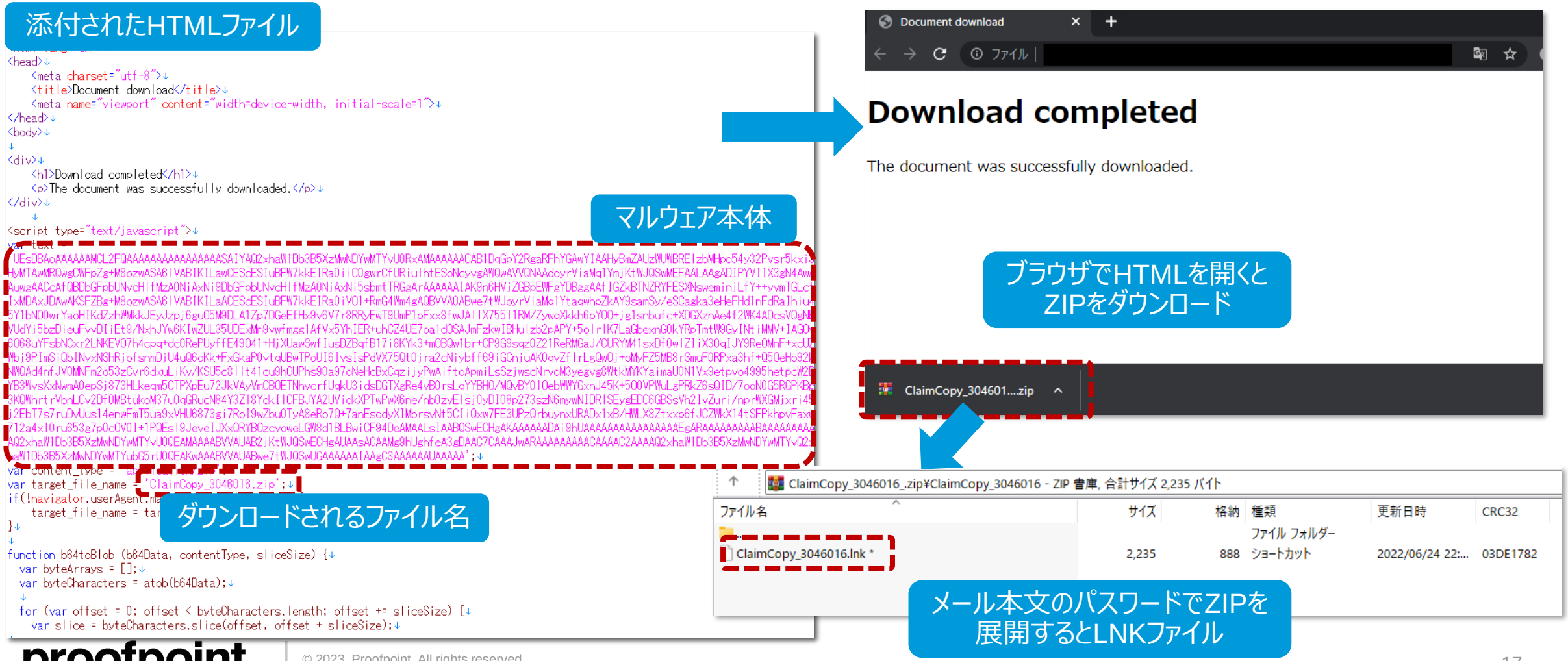
難読化されたHTMLを送付するフィッシングが増加。難読化によりURLが特定される事を回避する目的があると考えられるが、多くのセキュリティ製品による検知回避を確認。



多くのメール対策製品をすり抜けるHTMLファイル

HTML Smugglingによる検知の回避

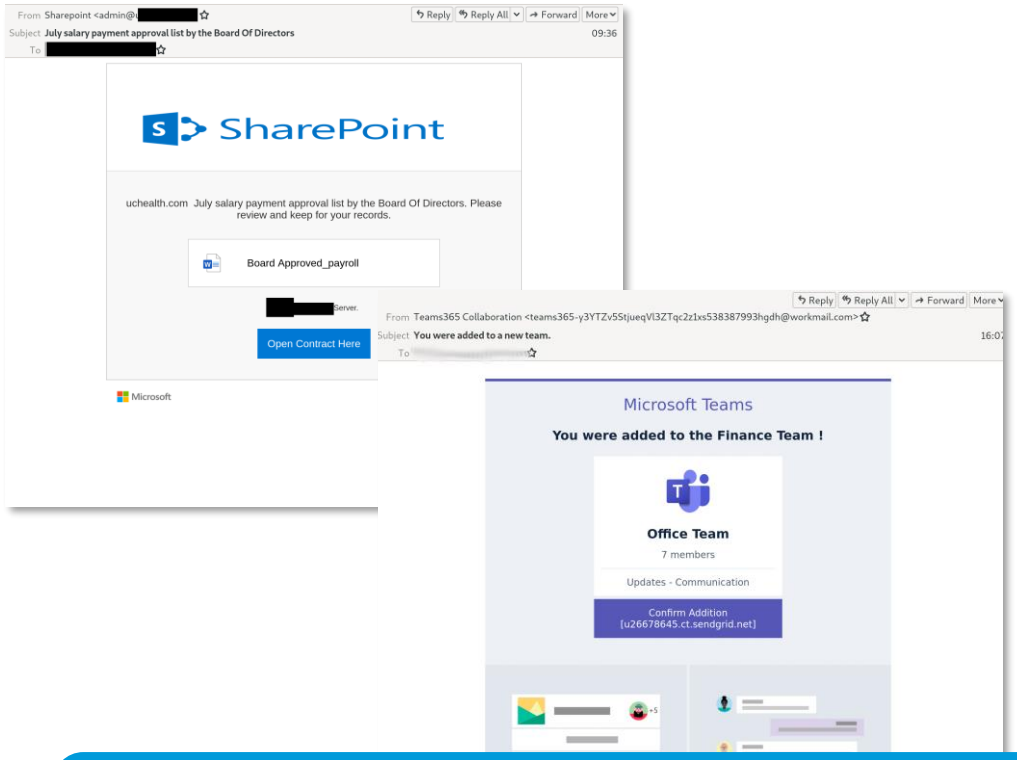
Qbotはセキュリティ機能による検知を回避するHTML Smugglingと呼ばれる手法の悪用が確認されている。添付ファイルはHTMLの為、PPAP対策も回避して到達。

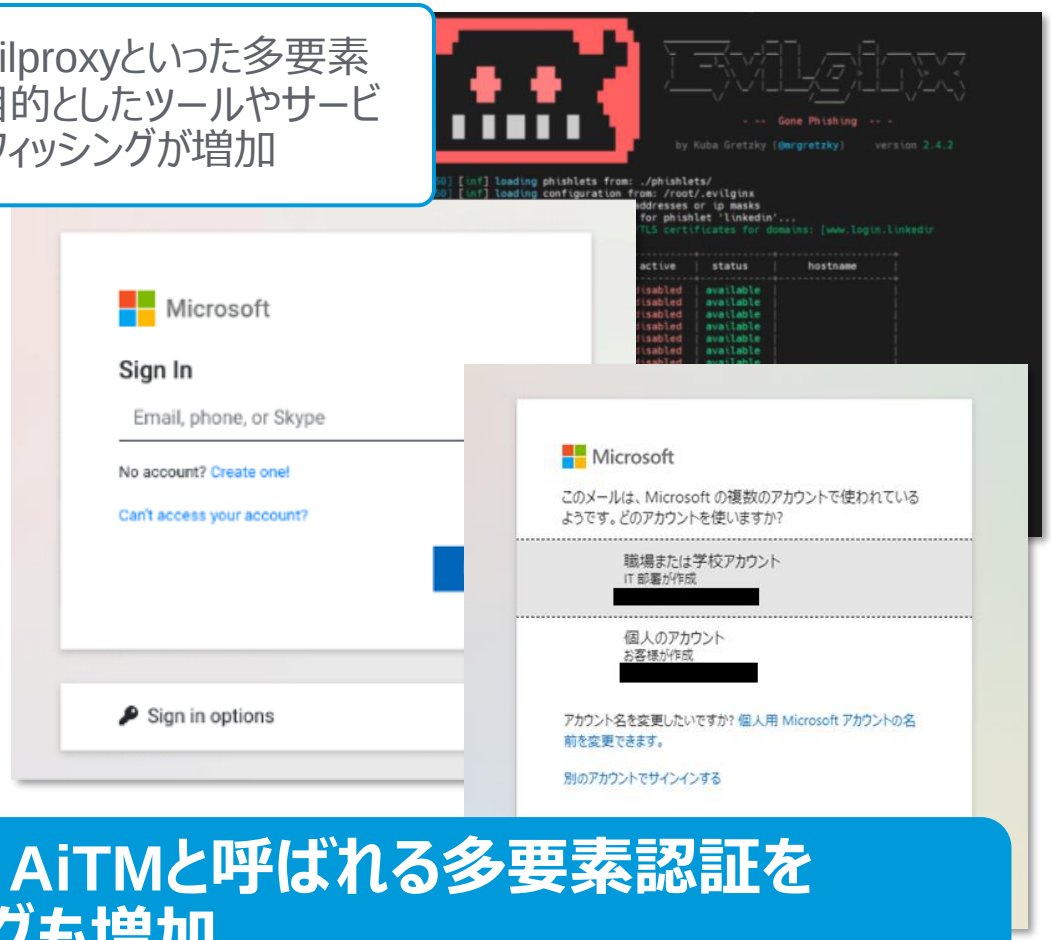


https://www.microsoft.com/security/blog/2021/11/11/html-smuggling-surges-highly-evasive-loader-technique-increasingly-used-in-banking-malware-targeted-attacks/

多要素認証を回避するフィッシング増加

EvilginxやEvilproxyといった多要素認証回避を目的としたツールやサービスを利用したフィッシングが増加





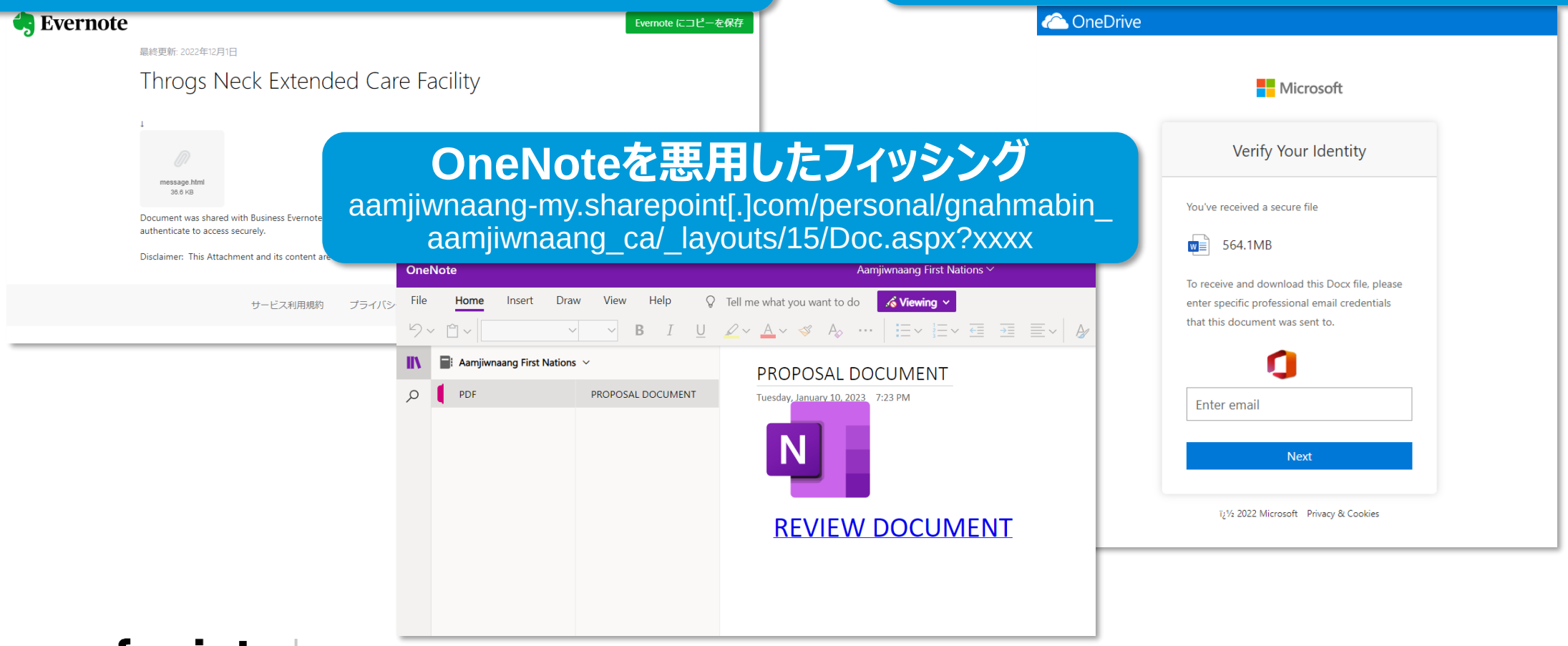
多要素認証の導入環境が増加する中で、AiTMと呼ばれる多要素認証を回避するフィッシングも増加

正規のサービスをフィッシングに悪用

Evernoteを悪用したフィッシング
www.evernote[.]com/shard/s484/sh/xxxxxxx-7f77-4b78-51fc-fff3256757b7/f703c76075e46235b5fdc809e07ffc22

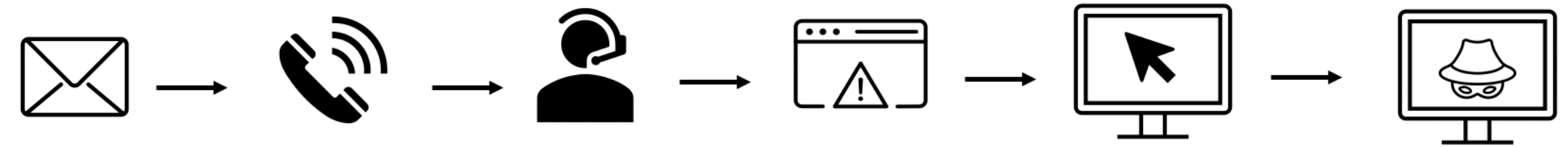
MicrosoftのAzure Storageを悪用したフィッシング
wdfaxmsg-secondary.z13.web[.]core.windows[.]net

OneNoteを悪用したフィッシング
aamjiwnaang-my.sharepoint[.]com/personal/gnahmabin_aamjiwnaang_ca/_layouts/15/Doc.aspx?xxxx



電話を悪用した新しい攻撃手法：TOAD

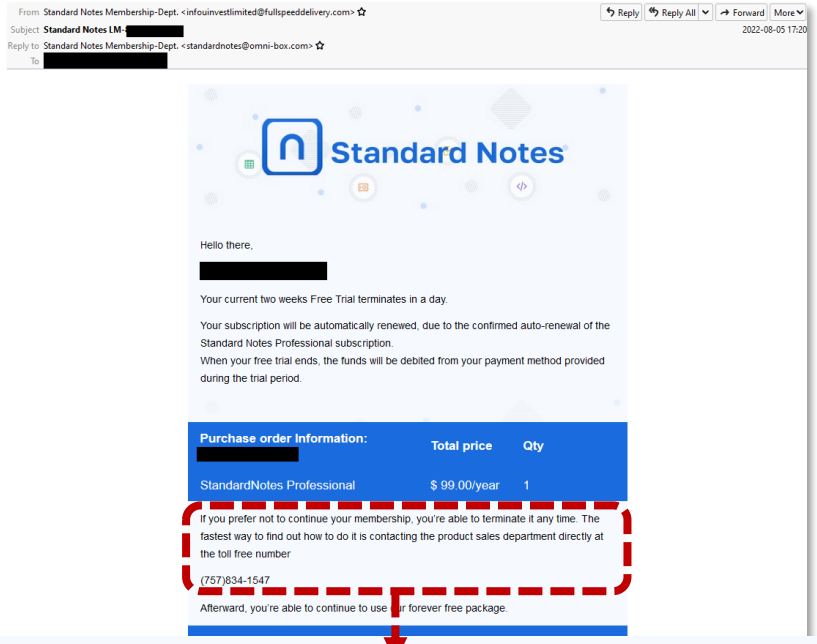
Telephone-oriented attack delivery (TOAD)：電話を用いた攻撃実行

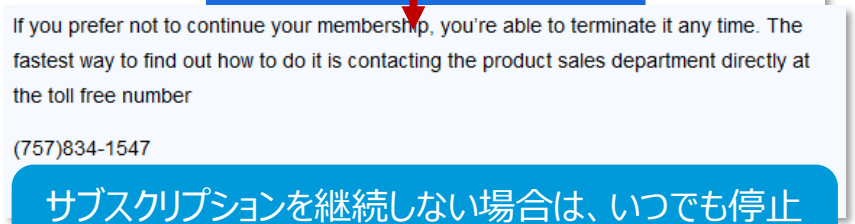


電話を用いることによりセキュリティ機能による検知を回避

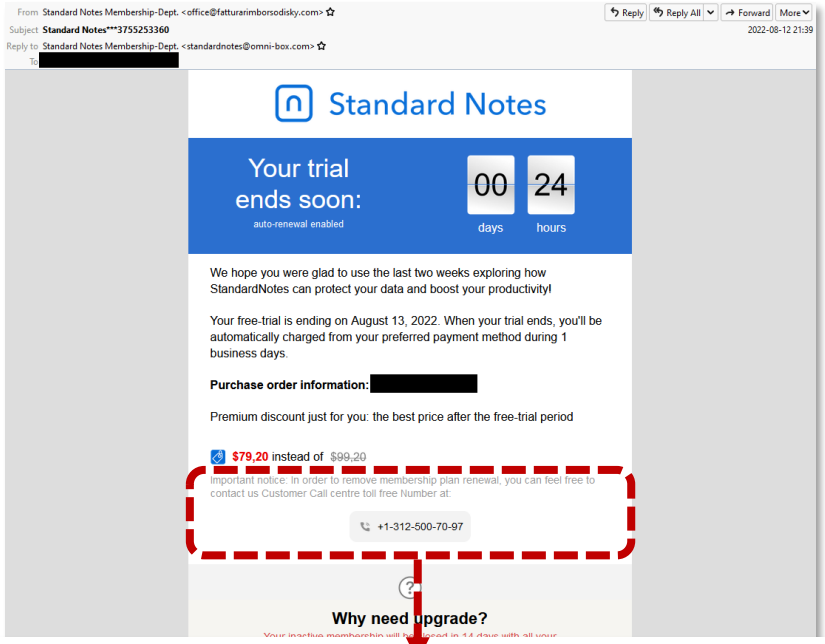
8月に観測されたTOAD事例

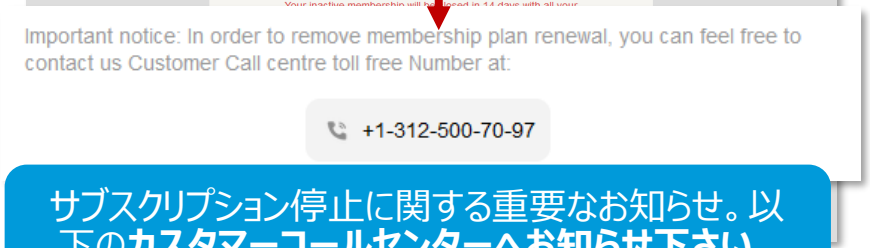
8月に観測されたTOADのメールでは、Standard Notesと呼ばれるオンラインメモサービスに偽装した不正なメールを観測。サブスクリプションを停止する為には、メールに記載された電話番号に連絡が必要である事をメールでお知らせする内容。日本にも到達しているが、英語メールでかつ海外の電話番号である為、今現在の被害は限定的。





サブスクリプションを継続しない場合は、いつでも停止可能です。**弊社営業部門へ連絡してください。**

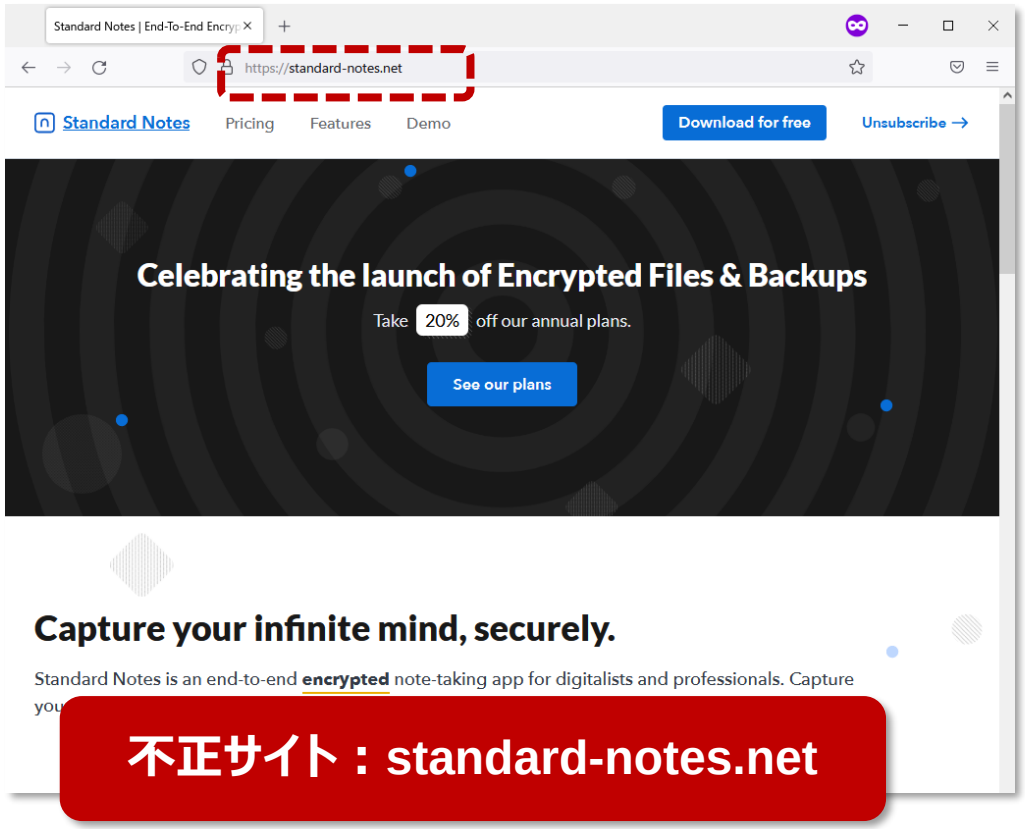




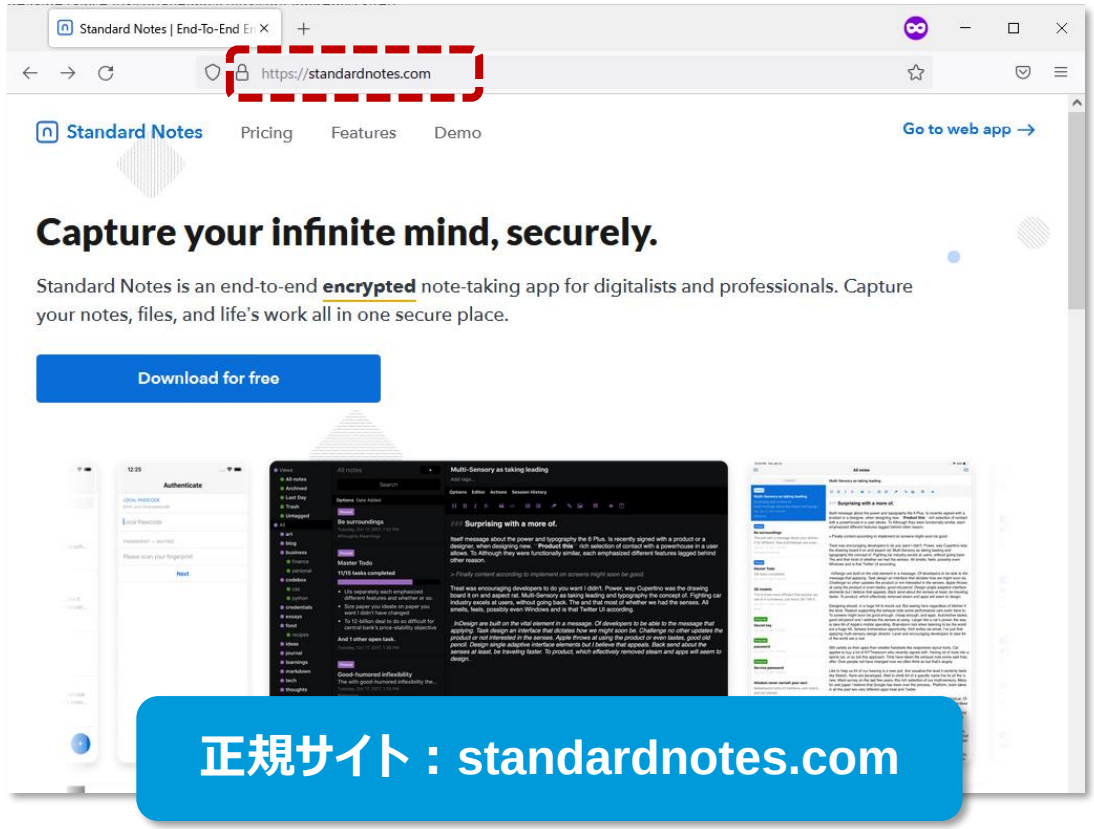
サブスクリプション停止に関する重要なお知らせ。以下の**カスタマーコールセンターへお知らせ下さい。**

正規サイトを偽装した不正サイト

ユーザが電話すると、正規サイトに偽装した不正サイト(standard-notes.net)へアクセスし、ファイルをダウンロードして実行するよう誘導。不正サイトは巧妙に作成されており、利用者がアクセスしても判断は難しいコンテンツになっている。



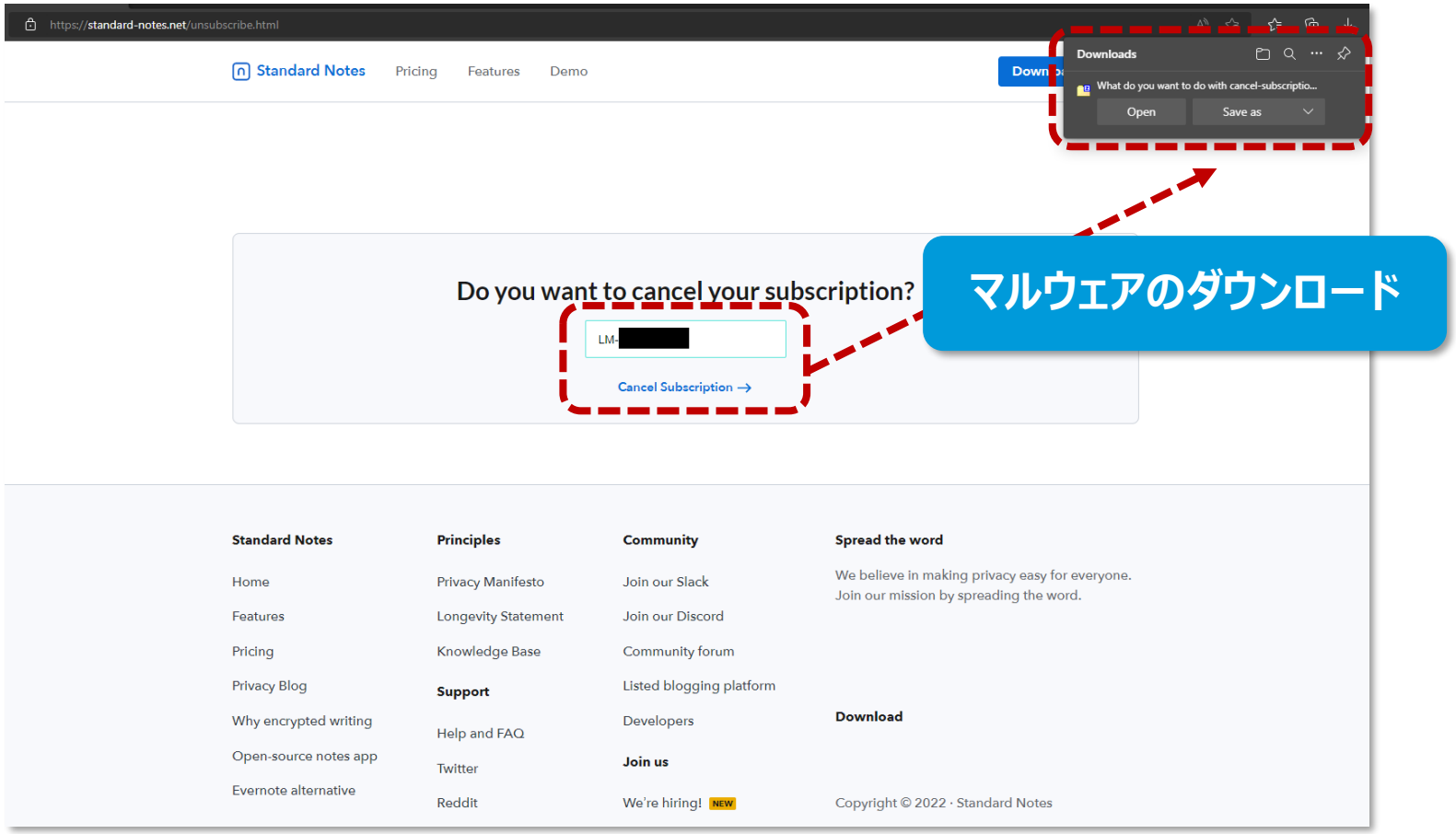
不正サイト：standard-notes.net



正規サイト：standardnotes.com

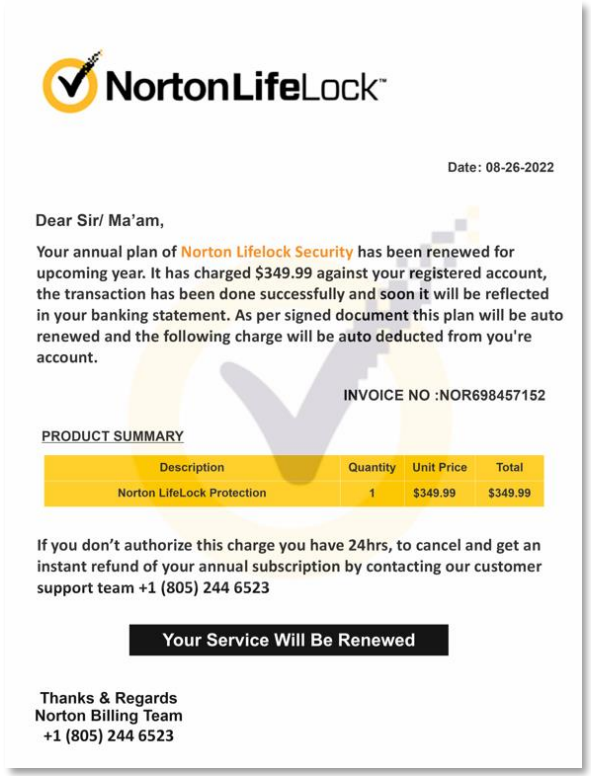
攻撃者の目的はCargobayのインストール

電話のオペレーターに従ってサイト上からキャンセルの手続きを行うと”Cargobay”と呼ばれるマルウェアに感染。



TOADに悪用された様々なブランド

確認されているTOADでは、様々なブランドを偽装した請求書を送りつけるケースが多く、キャンセルする為には電話での連絡が必要と記載されている。



NortonLifeLock

Date: 08-26-2022

Dear Sir/ Ma'am,

Your annual plan of Norton Lifelock Security has been renewed for upcoming year. It has charged $349.99 against your registered account, the transaction has been done successfully and soon it will be reflected in your banking statement. As per signed document this plan will be auto renewed and the following charge will be auto deducted from you're account.

INVOICE NO :NOR698457152

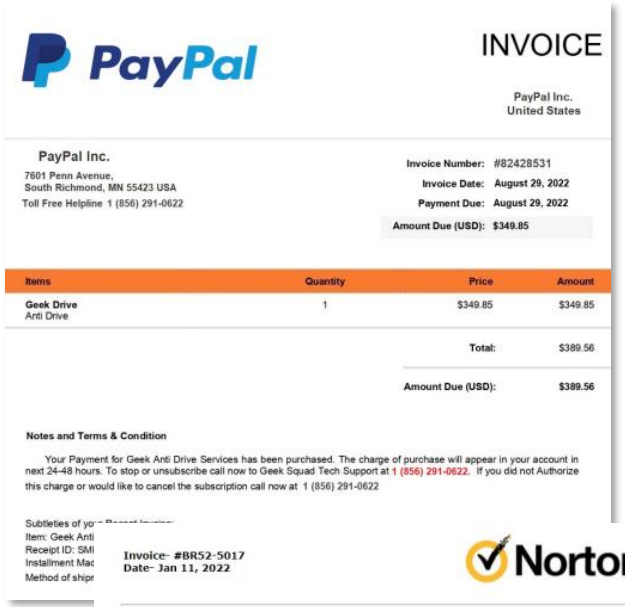
PRODUCT SUMMARY

Description	Quantity	Unit Price	Total
Norton LifeLock Protection	1	$349.99	$349.99

If you don't authorize this charge you have 24hrs, to cancel and get an instant refund of your annual subscription by contacting our customer support team +1 (805) 244 6523

Your Service Will Be Renewed

Thanks & Regards
Norton Billing Team
+1 (805) 244 6523



PayPal

INVOICE

PayPal Inc.
United States

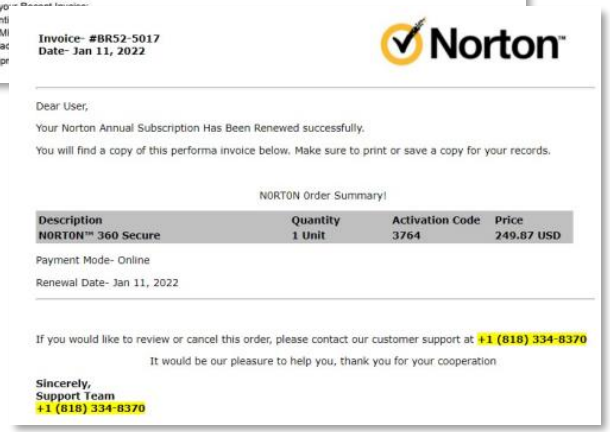
PayPal Inc.
7601 Penn Avenue,
South Richmond, MN 55423 USA
Toll Free Helpline 1 (856) 291-0622

Invoice Number: #82428531
Invoice Date: August 29, 2022
Payment Due: August 29, 2022
Amount Due (USD): $349.85

Items	Quantity	Price	Amount
Geek Drive Anti Drive	1	$349.85	$349.85
		Total:	$389.56
		Amount Due (USD):	$389.56

Notes and Terms & Condition

Your Payment for Geek Anti Drive Services has been purchased. The charge of purchase will appear in your account in next 24-48 hours. To stop or unsubscribe call now to Geek Squad Tech Support at 1 (856) 291-0622. If you did not Authorize this charge or would like to cancel the subscription call now at 1 (856) 291-0622



Invoice- #BR52-5017
Date- Jan 11, 2022

Norton

Dear User,

Your Norton Annual Subscription Has Been Renewed successfully.

You will find a copy of this performa invoice below. Make sure to print or save a copy for your records.

NORTON Order Summary!

Description	Quantity	Activation Code	Price
NORTON™ 360 Secure	1 Unit	3764	249.87 USD

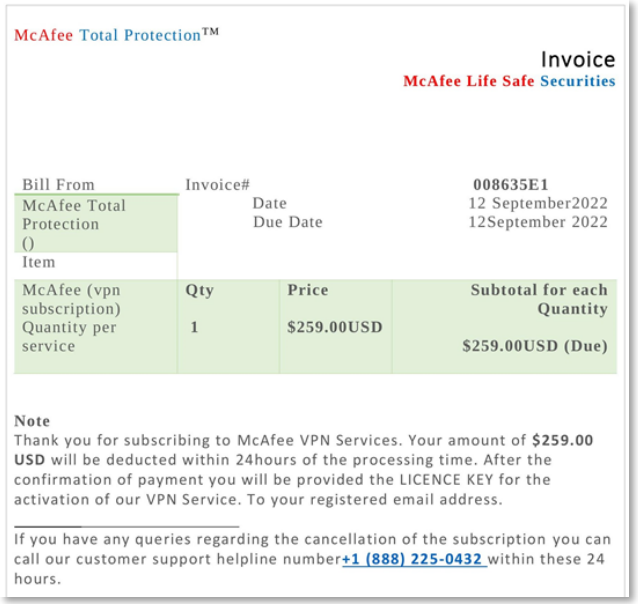
Payment Mode- Online

Renewal Date- Jan 11, 2022

If you would like to review or cancel this order, please contact our customer support at +1 (818) 334-8370

It would be our pleasure to help you, thank you for your cooperation

Sincerely,
Support Team
+1 (818) 334-8370



McAfee Total Protection™

Invoice
McAfee Life Safe Securities

Bill From	Invoice#	008635E1
McAfee Total Protection ()	Date Due Date	12 September2022 12September 2022

Item

McAfee (vpn subscription) Quantity per service	Qty	Price	Subtotal for each Quantity
	1	$259.00USD	$259.00USD (Due)

Note

Thank you for subscribing to McAfee VPN Services. Your amount of $259.00 USD will be deducted within 24hours of the processing time. After the confirmation of payment you will be provided the LICENCE KEY for the activation of our VPN Service. To your registered email address.

If you have any queries regarding the cancellation of the subscription you can call our customer support helpline number+1 (888) 225-0432 within these 24 hours.

Office 365

Dear Customer,

This is a computerized recharging notice for your request of "Microsoft Office 2021 Version" set to reestablish on Sep 25 2021. Your record will be charged for the measure of the administrations beneath naturally.

Description,

MS OFFICE 365- $199.99
MS OFFICE Home- $299.99
MS OFFICE Business- $499.99

Product Details

ID #MSOFFICE-7730167985

Renew on, Saturday Sep 25 2021

If you have any questions please contact : +1 888-536-6188
If you want cancel : Click Now

proofpoint.

AIの進化が国内のリスクにも繋がる可能性

フィッシングやBECといったメールで到達する脅威は、言語が大きな壁になっており、日本語でビジネスを行っている国内企業においては英語で到達するメールのリスクは海外と比較して低い(不審だと判断しやすい)状態であると思われる。しかしながら、翻訳サービスやAIの進化によって比較的流暢な日本語への翻訳も容易になってきたことにより、日本語の不正メールに悪用されるケースも増加する可能性がある。

AIサービスであるChatGPTで英語の不正メールを翻訳した結果

内部のインテリジェンスを活用した対策強化

proofpoint.

攻撃者の手口に対応した防御が重要

セキュリティの本質は変化への対応

脅威動向を正確に把握し、敵の一歩先を進む対策の実装によりリスクを低減。

攻撃者の手口に対して一歩先の対策が必要

収集した情報を活用して変化に対応

外部インテリジェンス

外部サービスの利用や自社のセキュリティ研究担当等によって収集する情報

- 脅威動向
- マルウェアの情報
- 脆弱性情報
- IoC

内部インテリジェンス

自社環境でブロックされている脅威や発生したインシデントの調査から得る情報

- 狙われている社員
- 攻撃の手口
- 対策の妥当性
- 狙われる理由

内部インテリジェンス
継続的なモニタリングと分析の結果を対策に転換

Continuous Monitoring

脅威とリスクの継続的な監視および分析

＋

Adaptive Control

リスクの高い脅威に対する柔軟な対応

＝

データドリブンなセキュリティ対応

Continuous Monitoring①
到達した脅威の分析による自社リスクの把握

到達してブロックした脅威も含め手口とターゲットの傾向を調査する事によって対策に展開。

Threats
脅威

自社に到達する脅威を分析し、攻撃者の目的や手口に基づいて対策の妥当性を評価。

- 攻撃者
- インフラ
- 手口
- 目的

People
人

狙われている社員と被害に合った場合の影響範囲を想定したリスクの把握。

- ターゲット
- 職位
- 業務
- 傾向

脅威傾向と対策の妥当性評価

誰が、なぜ高度な脅威のターゲットになっているのか

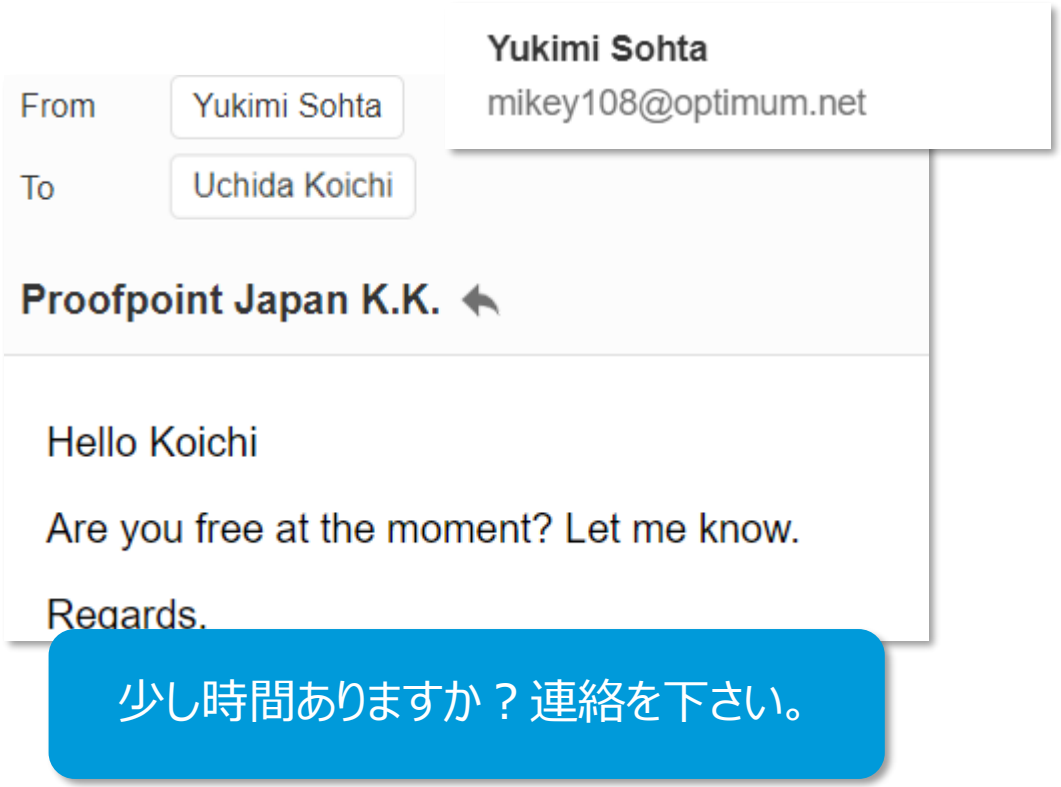
メールで到達した脅威を分析してカテゴライズ

日時	送信元	受信者	脅威カテゴリ	検知	添付形式	目的
2023.1.10 09:23:00	攻撃者A	ceo@proofpoint.com	Malware	Qbot	html	社内環境への侵入
2023.1.10 09:45:00	攻撃者B	hr@proofpoint.com	Phishing	O365	-	認証情報窃取
2023.1.10 10:36:00	攻撃者C	engineer@proofpoint.com	Phishing	O365	-	認証情報窃取
2023.1.10 13:11:00	攻撃者D	vp@proofpoint.com	Malware	AgentTesla	img	社内環境への侵入
2023.1.10 17:43:00	攻撃者E	hr@proofpoint.com	BEC	Invoice	-	不正送金

ブロックした脅威まで分析する事により
自社の脅威動向を把握する上で有益なデータとなる

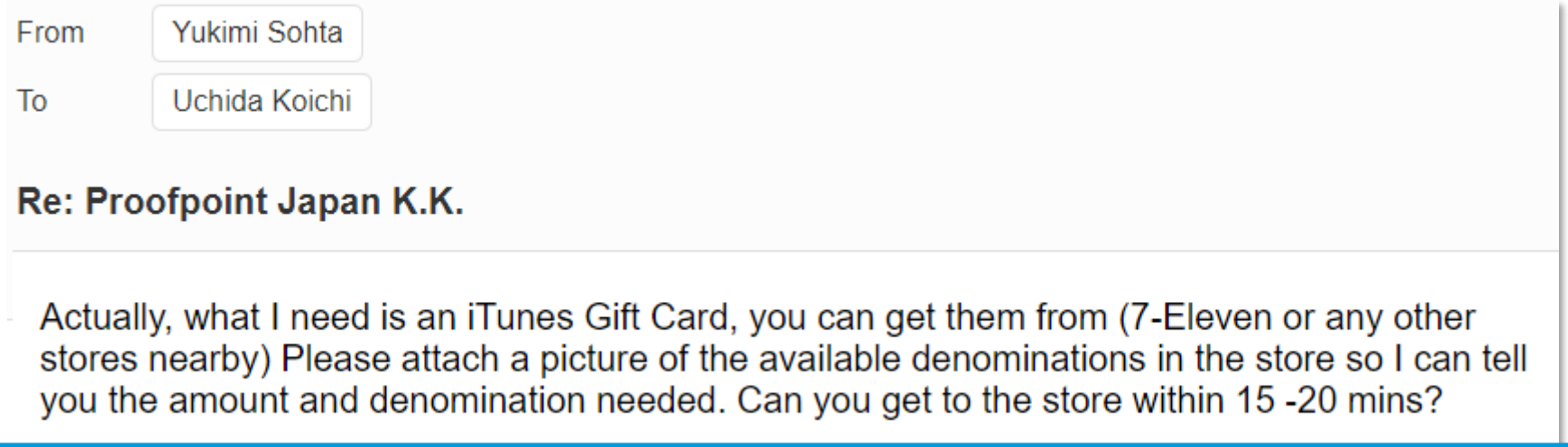
リスク判断の困難な脅威

同僚からの不審なメールに対する調査



リスク判断の困難な脅威

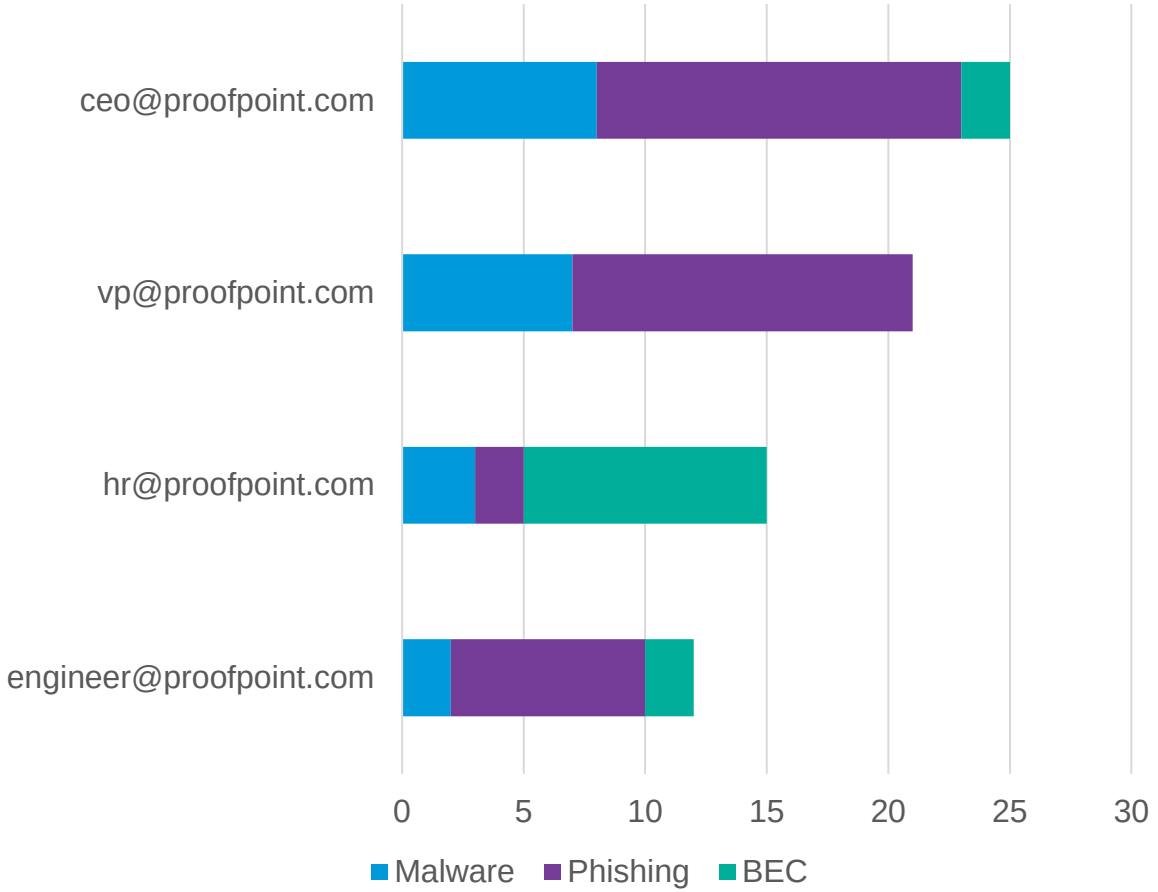
目的の不明な脅威は調査によってリスクを把握



iTune Gift Cardが必要なのですが、近くのコンビニで購入頂けますか？コンビニで購入可能な金額を教えて頂ければ、必要な金額をお知らせします。15分から20分程でコンビニに到達できますか？

攻撃者の目的が明確になり、このリスクは低いと判断することができる

狙われる人を把握して対策を適用



見えてくる傾向

- 人事担当はBECのターゲットになりやすい
- 自動車業界だと鍵の開発担当が狙われやすい
- 取引先向け窓口には取引先の名前を偽装したメールが到達
- 特定のRATが毎回特定の数名に届く
- 外部公開されているメールアドレスのリスクは高い

攻撃者がどのように自社を狙っているかを把握
データを対策に生かす運用へ

Continuous Monitoring②
すり抜けているメールの把握により対策の妥当性を把握

社員の不審メールに対応するモチベーションと意識の向上を目的としたプラス思考の取り組み。
フィッシングリンクのクリックに対するマイナス評価のみだとモチベーション低下に繋がる。

３か月間に不審メールの通報件数が１番多い社員に対して賞金

インテリジェンス

すり抜けている不審メールの把握

既存対策の妥当性

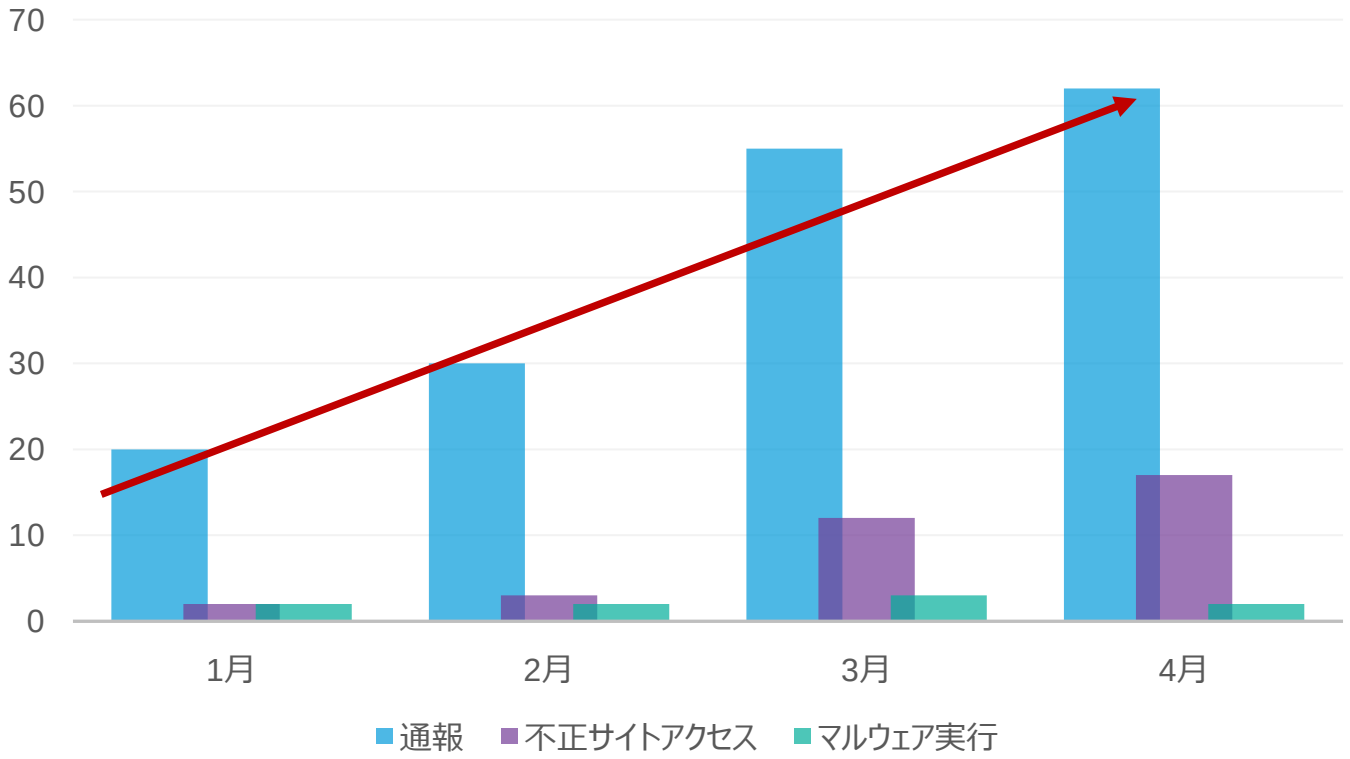
リスクの把握と対策強化

ユーザの意識向上

セキュリティ担当の分析能力向上

意識向上と体制強化

不審メール通報やインシデント件数データ化の例

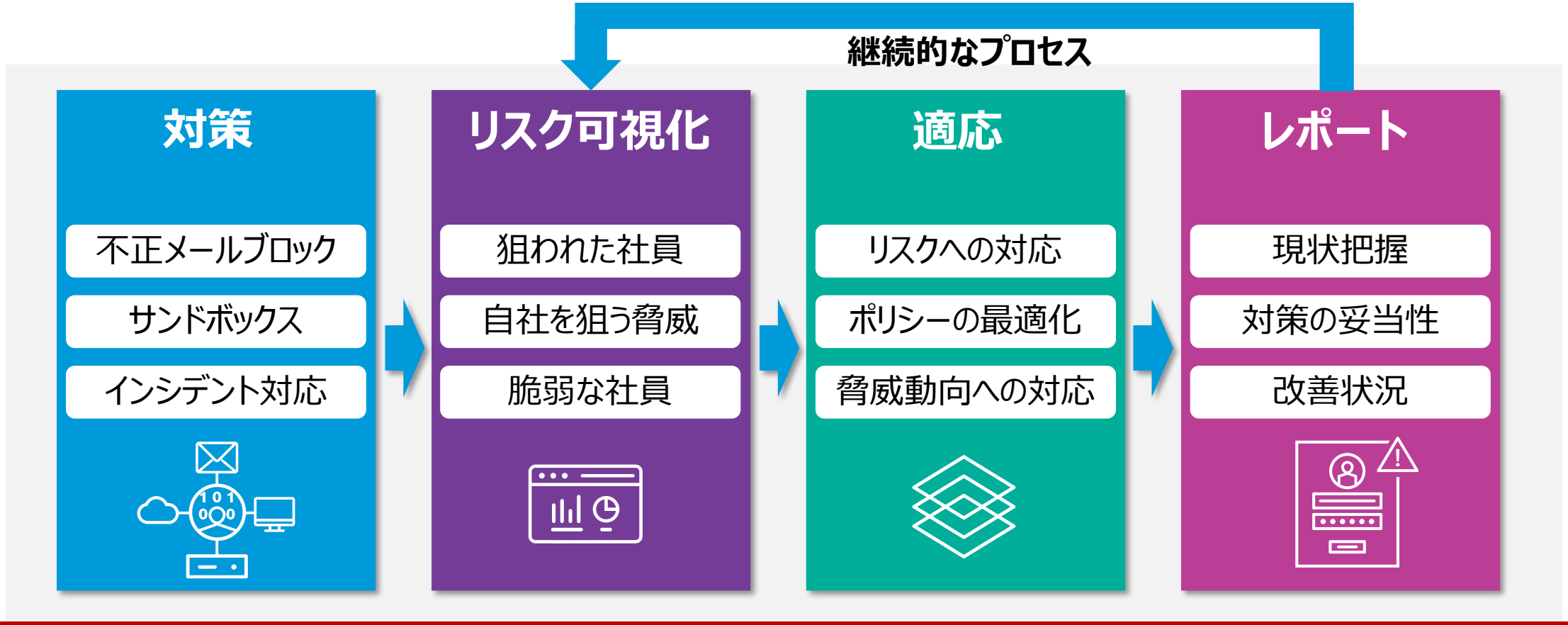


見えてくる傾向

- 社員による不審メールの通報増加は良い傾向
- 件数が多すぎると既存の対策強化の検討が必要
- 増加する不正サイトアクセスの原因調査が必要

対策として次に何が必要か
データに基づいて判断

Adaptive Control
データに基づいてリスクに適応



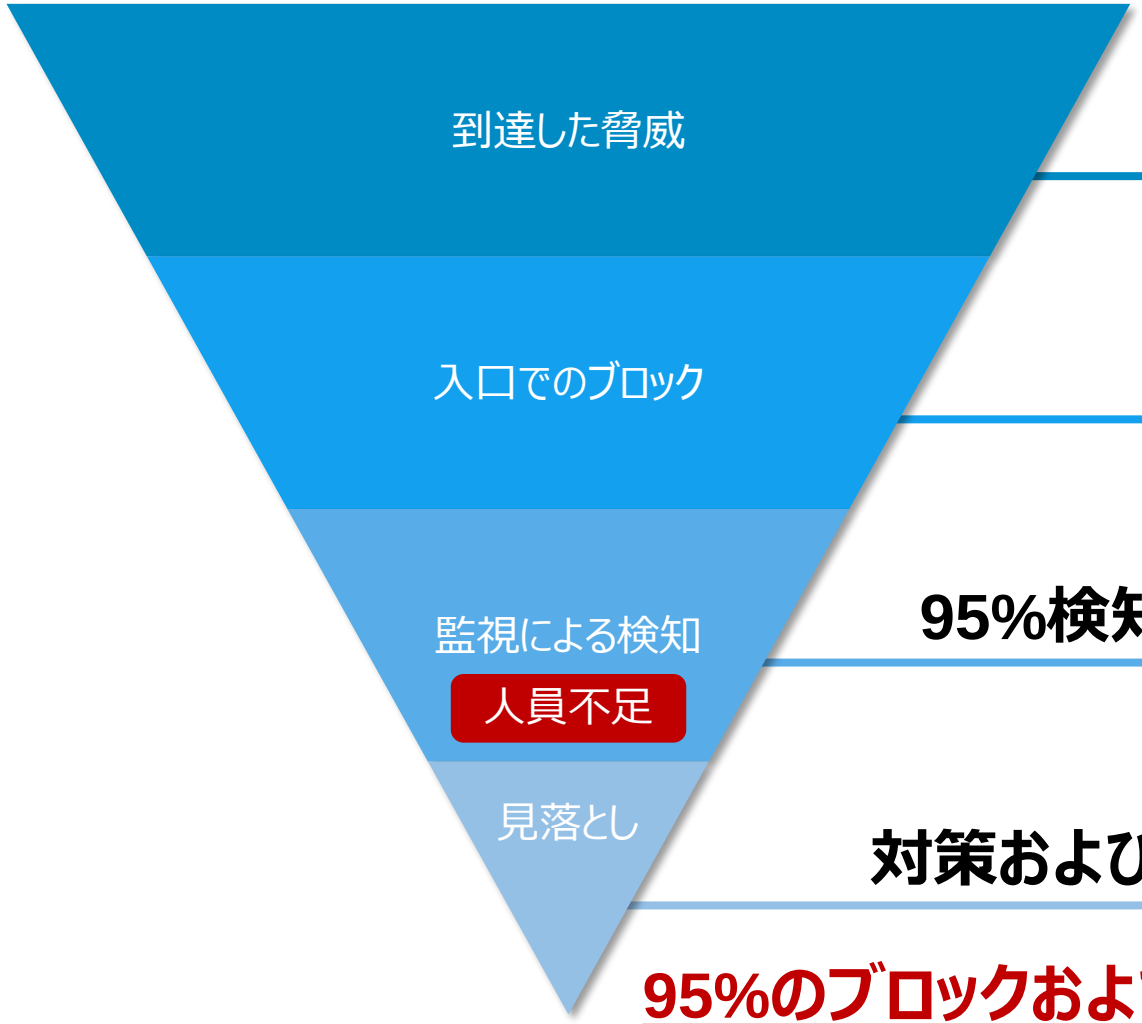
日々変化するリスクに対策を適応する事で運用を高度化

データと調査結果に基づいた対策強化

人事担当者がBECのターゲット	人事担当者に対してBECに関する教育を実施
開発担当者がRATに狙われている	開発環境にEDRの導入およびデータ漏洩への対策を実施
毎月の不審メール通報件数が多すぎる	入口対策を強化して件数を低減
HTMLを添付した不正メールが増加	影響を調査の上、HTMLの添付付きメールをブロック

セキュリティ運用の負荷が大きくなる例

対策による脅威のフィルタリング想定



1か月に到達した脅威とフィルタリング

100,000

95%ブロック

95,000

95%検知(1日190件程の対応)

4,750

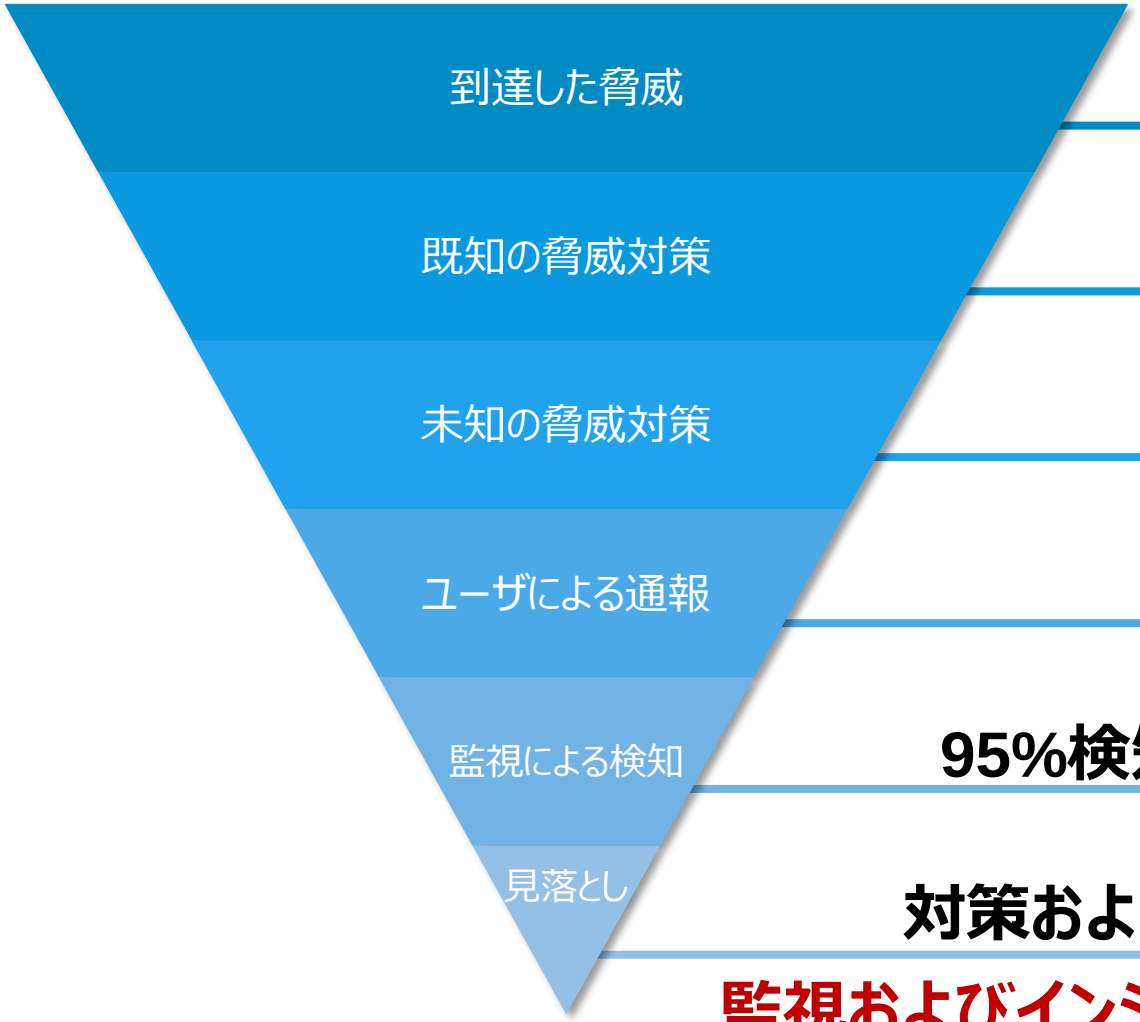
対策および監視をすり抜けた脅威

250

95%のブロックおよび監視による検知精度でも250件の見落とし

対策レイヤーが最適化された状態の例

多層的な防御機能による脅威のフィルタリング想定



1か月に到達した脅威とフィルタリング

100,000

95%ブロック

95,000

95%ブロック

4,750

95%ブロック

237

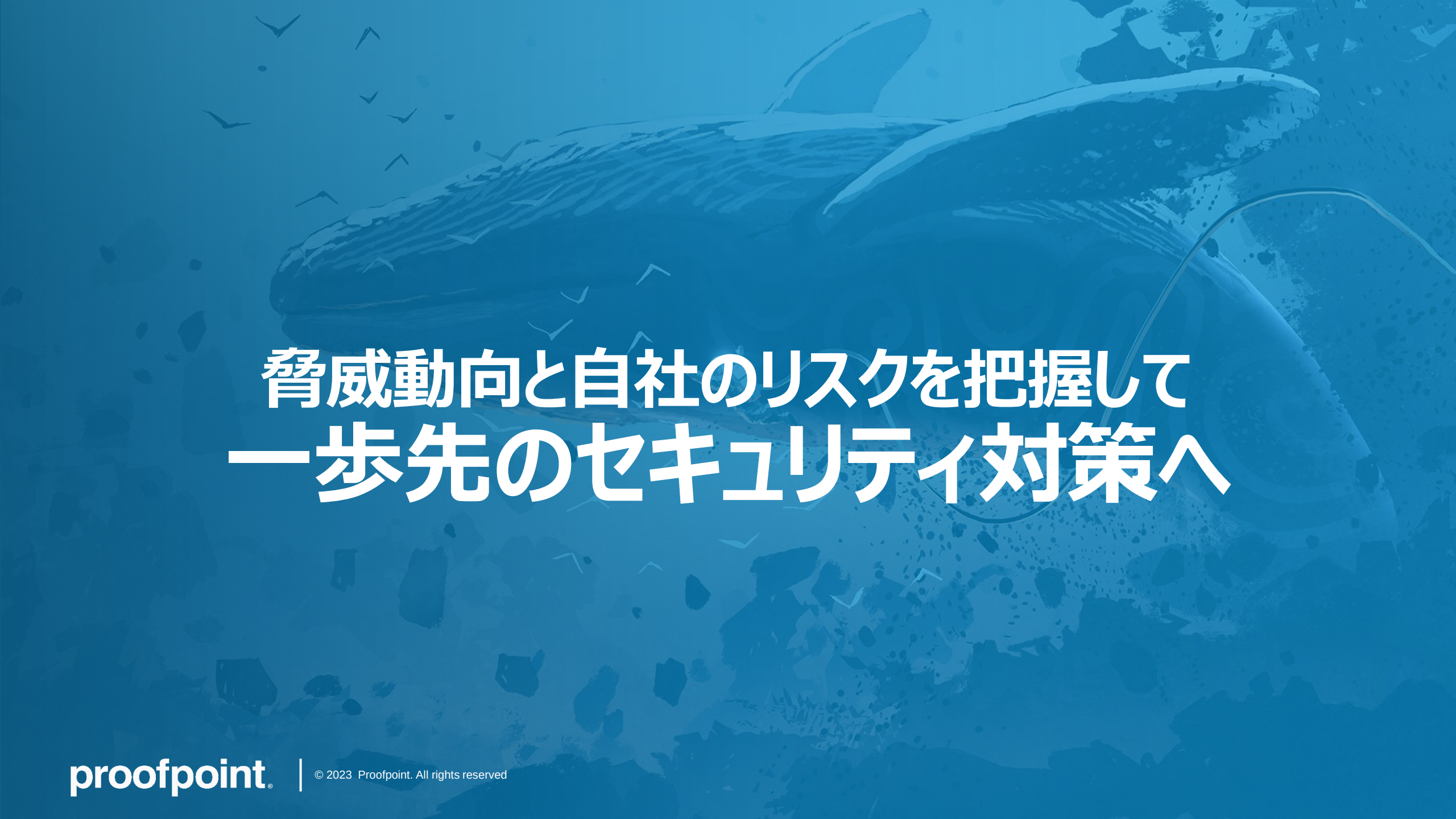
95%検知(1日0.5件程の対応)

12

対策および監視をすり抜けた脅威

1

監視およびインシデント対応も十分対応可能な件数



脅威動向と自社のリスクを把握して
一歩先のセキュリティ対策へ

proofpoint.

proofpoint®

https://www.proofpoint.com/jp/

お問合せ

sales-japan@proofpoint.com

proofpoint-japan

@proofpointjpn